

**ESTRUCTURA ARQUITECTÓNICA PARA LA IMPLEMENTACIÓN
DE LA LEY HABEAS DATA EN EL SECTOR FINANCIERO
COLOMBIANO**

LAURA MARCELA GONZÁLEZ CANO

**Trabajo de grado presentado como requisito parcial para optar al título de
Magíster en Ingeniería**

Asesor: Ph. D. JUAN GUILLERMO LALINDE PULIDO

**UNIVERSIDAD EAFIT
ESCUELA DE INGENIERÍA
MAESTRÍA EN INGENIERÍA
MEDELLÍN
2009**

Nota de aceptación

Presidente del Jurado

Jurado

Jurado

Medellín (Antioquia). 23 de noviembre de 2009.

A mi hermana, una brillante ingeniera.

RESUMEN

Arquitectura empresarial, metodologías y SOA

Las organizaciones actuales quieren potenciar su fuerza de negocio a través de la implementación de una arquitectura empresarial que provee una manera de ordenar todos los niveles de la empresa dentro de un marco de trabajo claramente definido que involucra todos los actores de la organización, centrándose en los procesos para alcanzar las estrategias y metas del negocio; es decir, que permite generar una estructura coherente entre los objetivos del negocio, la información, las aplicaciones y la tecnología.

¿Es posible implementar en las empresas colombianas actuales una arquitectura empresarial? Indudablemente el camino a penas comienza: Muy pocas organizaciones colombianas tienen definidos procesos integrados y congruentes con las metas del negocio. La naturaleza de las organizaciones son estructuras en silos, con esquemas de integración débiles y difícilmente mantenibles, lo que implica a las organizaciones que desean potenciarse a través de una arquitectura empresarial asumir el reto de trazar un camino de crecimiento y transformación para poder alcanzar un nivel de madurez que le permita lograr una alineación entre los objetivos estratégicos y todos los entes que conforman la organización comenzando por los procesos y terminando con la tecnología que los soporta.

La implementación de una arquitectura empresarial puede basarse en diferentes metodologías de referencias existentes como son TOGAF [1], Zachman [2], XAF [3], entre otras, las cuales son seleccionadas dependiendo de las necesidades. Básicamente definen como se deben realizar iteraciones entre diferentes dominios que permiten obtener una visión 360° de la organización y asegurarse que la tecnología apoya a la justa medida la estrategia del negocio. Los dominios pueden variar dependiendo de la metodología seleccionada, pero a nivel general se basa en una vista o dominio de negocio, información y tecnología.

La metodología de arquitectura empresarial brinda las herramientas para que se pueda definir un marco de trabajo que cubre toda la organización, pero a nivel de tecnología es especialmente relevante la definición de los servicios que debe proveer al negocio para apoyar la ejecución de los procesos y es en este punto dónde se introduce el concepto de Arquitecturas Orientadas a Servicios,

comúnmente denominada SOA. SOA permite definir e implementar servicios requeridos por un proceso de negocio y desplegarlos a partir de una infraestructura tecnológica. Para seguir un esquema ordenado de descubrimiento de servicios, es posible basarse en las definiciones de la metodología RUP/SOMA [11] para este fin.

Trabajo de Investigación

El trabajo de investigación, “Estructura Arquitectónica para la Implementación de la Ley Habeas Data en el Sector Financiero”, toma las mejores prácticas de Arquitectura Empresarial y SOA de la industria para ser una guía de referencia de las entidades financieras que se ven en la obligación de implementar requerimientos de ley, como es el caso de Habeas Data.

Al ser un marco que pretende ser implantado en todo un sector, la definición de la arquitectura de negocio y tecnología no puede orientarse por unos objetivos estratégicos particulares, por lo cual el trabajo se orienta a las necesidades a las que debe responder una organización independientemente de su estructura interna brindando una orientación metodológica para la implementación de servicios específicos que se integren a sus propios procesos de negocio.

El despliegue del marco arquitectónico objeto del presente trabajo de investigación, se encuentra estructurado de la siguiente manera:

1. Visión del proyecto

Define el alcance y producto que se obtiene del trabajo de investigación. La visión del proyecto es un artefacto que permite definir el producto que se desea obtener bajo unas condiciones específicas para la ejecución del proyecto.

El trabajo de investigación, “Estructura Arquitectónica para la Implementación de la Ley Habeas Data en el Sector Financiero”, se basa en las mejores prácticas definidas en las metodologías para arquitectura empresarial TOGAF, XAF y RUP-SOMA lo cual permite establecer una rápida adaptación de los procesos de la organización con el mínimo impacto sobre la infraestructura tecnológica actual de la entidad financiera a través de la definición de una Arquitectura de negocio, para poder definir los procesos genéricos que afectan

la implantación de la ley; arquitectura de información, para la definir los datos de entrada y salida requeridos para la ejecución de los procesos; arquitectura de aplicación, en la que se realiza un descubrimiento de los servicios que se soportan los procesos de negocio y; por último, la arquitectura tecnológica, que presenta alternativas de infraestructura SOA que la entidad financiera puede considerar para realizar el despliegue de los servicios definidos.

El modelamiento de la arquitectura de referencia se realiza bajo el concepto MDA [17] (Model Driven Architecture) el cual garantiza que el diseño arquitectónico pueda ser usado por cualquier entidad, ya que se generan Modelos Independientes de la Plataforma (Platform-Independent Model o PIM) que posteriormente, puedan ser adaptados por una organización específica y mapeados a su infraestructura particular, creando modelos de plataforma específica (Platform-Specific Model o PSM). [17].

2. Arquitectura de negocio:

Una arquitectura de negocio permite reconocer desde diferentes vistas, cual es el impacto que tiene para una organización la implementación de un nuevo requerimiento, como es la Ley Habeas Data en las entidades financieras colombianas.

Para poder determinar de manera genérica el impacto que genera la implementación de la ley en un sector financiero y no en una organización específica, fue necesario definir el contexto de nuestras organizaciones actuales, validar que procesos y sistemas de información indispensables dentro de estas organizaciones para poder prestar servicios financieros bajo las reglamentaciones vigentes.

Posteriormente, con el apoyo de un grupo multidisciplinario, se realiza un análisis detallado de la ley para definir los requerimientos y estimar cuales tienen un impacto a nivel de proceso y/o tecnología para una empresa del sector financiero. Una vez definidos los requerimientos, se comienza a generarse vistas del negocio en las cuales se definen las restricciones y principios arquitectónicas, el diagrama de contexto, la definición de los procesos usando el estándar notacional de BPMN (Notación para el modelado de procesos de negocio - Business Process Management Notation) [41] avalado por la OMG [21], para que la lectura de esos procesos no esté sujeta a

personalizaciones; y por último, es la vista organizacional, para definir los roles necesarios que debe tener la entidad financiera para poder realizar los procesos Habeas Data.

Cabe aclarar que esta arquitectura define el proceso de negocio compuesto de actividades operativas o automáticas; es decir, tareas que se ejecutan manualmente o a través de un servicio que sea publicado por un sistema de información. Lo importante es poder definir que es lo que debe realizarse y a partir de este entregable, las arquitecturas subsiguientes, definen la naturaleza de los servicios candidatos que pueden ser publicados por la entidad para la ejecución de su proceso.

3. Arquitectura de información:

La correcta gestión de la información crediticia es el punto neurálgico que constituye la Ley Habeas Data, por lo cual el principal punto de discusión al afrontar la Arquitectura de información es poder responder que datos son necesarios para ejecutar los procesos determinados en la Arquitectura de Negocio a través de Modelos Canónicos de Datos; es decir, definir los datos de manera genérica para que sea independiente a cualquier tipo de plataforma tecnológica. Pero no basta con definir cuales es la información requerida, sino que esa información debe tener un Ciclo de Vida dentro de la organización, para lo cual se deben generar políticas administrativas que permitan establecer la temporalidad que debe tener la información en cada procedimiento Habeas Data.

Cuando una entidad financiera específica, transforme el modelo canónico a las entidades de información implantadas, debe determinar necesidades de integridad de información que pueden ser resueltas a través de adaptadores implementados en un Bus de Servicios, pero por ser el trabajo de investigación un marco genérico para el sector, no está dentro del alcance realizar un estudio específico de la naturaleza de cada organización que use el marco para poder implementar la ley Habeas Data de manera consistente y oportuna.

4. Arquitectura de servicios:

La definición y el modelado de servicios es el corazón de una Arquitectura Orientada a Servicios (SOA).

La arquitectura de servicios tiene como objetivo realizar descubrimiento del portafolio de servicios que responden a los procesos Habeas Data, categorizarlos y definir el flujo de mensajes entre ellos. Es importante aclarar, que el resultado de esta arquitectura es orientar a la organización financiera sobre los servicios que debería desplegar en su infraestructura SOA, determinando los flujos, las dependencias y las composiciones de los servicios que soportan los procesos; siendo aún un modelado independiente de la plataforma.

5. Arquitectura técnica:

La implantación de la Estructura Arquitectónica para la Implementación de la Ley Habeas Data en el Sector Financiero, tiene precondiciones de tecnología como es contar con una plataforma SOA, pero no se realiza ningún tipo de modelado bajo el enfoque de alguna de infraestructura SOA disponibles en el mercado de tecnología. Para el alcance del proyecto de investigación, se presenta al lector un acercamiento de los componentes que conforman las plataformas SOA mejor posicionadas en el mercado según el cuadrante mágico de Gartner [42], pero en ningún momento se orienta o se impone la utilización de alguna en particular.

Es en la arquitectura técnica en dónde la entidad financiera que use el marco de referencia dispuesto en este trabajo de investigación, realiza personalización de los procesos y servicios, toma decisiones de integración y realiza modelado arquitectónico dependiente de la plataforma en dónde realizará el despliegue, siguiendo el marco de modelado de MDA [17] utilizado para realizar las definiciones de los modelos durante el ciclo de vida de implementación de servicios.

Ley 1266 de 2008, Habeas Data

Es la ley por la cual se dictan las disposiciones generales y se regula el manejo de la información personal, crediticia, financiera y comercial contenida en las bases de datos de las Centrales de Riesgo (Cifin y Datacrédito), con el objetivo de desarrollar el Derecho Constitucional que tienen todas las personas a conocer, actualizar y solicitar rectificación de la información que se haya recogido sobre ellas en los Bancos de datos. [7].

1. Información Financiera

Las entidades financieras deben enviar a las Centrales de Riesgo el Reporte Positivo (cuando las personas están al día en sus obligaciones) y el Reporte Negativo (cuando las personas naturales o jurídicas efectivamente se encuentran en mora en sus cuotas u obligaciones).

La permanencia de la información será administrada exclusivamente por las Centrales de Riesgo.- Cifin y Datacredito. La información de carácter positivo permanecerá de manera indefinida, mientras la permanencia de la información negativa se calcula de la siguiente manera:

- Para las obligaciones con Mora Inferior a 2 años, la información permanecerá por un periodo correspondiente al doble de la mora.
- Para las obligaciones con Mora Superior a 2 años, se almacenará por un periodo de 4 años a partir de la fecha de pago de la obligación
- Obligaciones Insolutas: La información negativa de obligaciones insolutas o no pagadas, solo permanecerá por diez (10) años, posterior a este plazo será eliminado el reporte en centrales de riesgo, pero la deuda y los procesos legales sobre la misma seguirán vigentes.

2. Deberes y obligaciones de las entidades financieras

- Garantizar la calidad y veracidad de la información al momento de la creación y modificación de las obligaciones en cada uno de los sistemas.
- La consulta a las centrales de riesgo solo podrá realizarse siempre que exista la autorización por parte del titular (cliente o no cliente de la entidad) y para los fines establecidos en los procedimientos internos de la entidad financiera.
- La consulta a las centrales de riesgo solo podrá realizarse por los funcionarios que posean clave personal otorgada por las centrales de riesgo.
- Reportar periódica y oportunamente a las Centrales de Riesgo el comportamiento mensual, las novedades de las obligaciones y de rectificar la información cuando esta sea incorrecta.
- Resolver los reclamos y peticiones de los titulares referentes a la información reportada en centrales de riesgo.
- El reporte de información negativa que hagan las fuentes de información a las centrales de riesgo, sólo procederá previa comunicación al titular de la información, para lo cual la entidad financiera deberá enviar comunicación al cliente informando que se encuentra en mora. Dicha comunicación será enviada los primeros días del mes. Una vez transcurridos veinte (20) días calendario siguientes a la fecha de envío de la comunicación en la última dirección de registrada por el titular, la entidad financiera podrá reportar la información del cliente a las Centrales de Riesgo.

3. Régimen de sanciones

El incumplimiento de las entidades financieras a los deberes estipulados en la Ley 1266- Habeas Data, generará multas de carácter personal e institucional por parte de la Superintendencia Financiera de Colombia hasta por el equivalente a mil quinientos (1500) salarios mínimos mensuales legales vigentes.

Contenido

1	Introducción.....	24
2	Visión del proyecto	25
2.1	Posicionamiento del proyecto	25
2.1.1	Definición del problema.	25
2.1.2	Objetivos del proyecto	26
2.1.3	Definición del posicionamiento del producto	27
2.2	Descripción de interesados.....	29
2.2.1	Sumario de involucrados a nivel corporativo.	29
2.2.2	Sumario de involucrados a nivel de proyecto	30
2.2.1	Ambiente de usuario.....	33
2.3	Descripción del producto	36
2.3.1	Perspectiva del producto..	36
2.3.2	Supuestos y dependencias.....	38

2.3.3	Necesidades y características.	38
2.4	Atributos de calidad	52
3	Arquitectura de negocio	53
3.1	Representación arquitectónica	53
3.2	Conductores arquitectónicos	53
3.2.1	Objetivos arquitectónicos	54
3.3	Restricciones arquitectónicas	55
3.3.2	Principios Tecnológicos.	56
3.2.3	Principios de arquitectura para el proyecto.	61
3.3	Vista de mercado	63
3.3.1	Marco de negocio.	63
3.3.2	Contexto de negocio	65
3.4	Vista de proceso de negocio.....	67
3.4.1	Procesos del negocio impactados por el proyecto.....	68
3.4.2	Macroproceso para la ejecución de la Ley Habeas Data.....	72
3.4.3	Proceso: Comunicación a clientes morosos	76
3.4.4	Proceso: Generación diaria de archivos de pagos.....	88

3.4.5	Proceso: Novedades de los reportes a las centrales de riesgo	94
3.4.6	Proceso: Marcación de reclamos en las centrales de riesgo	103
3.5	Vista de organizacional.....	114
3.5.1	Responsabilidades equipo de ejecución del proyecto	114
3.6	Vista de recursos humanos	116
3.6.1	Equipo para la ejecución de procesos	116
4	Arquitectura de información.....	118
4.2	Vistas de arquitectura de información.....	118
4.3	Ciclo de vida de la información	119
4.4	Modelo canónico de datos	123
4.4.1	Proceso: Comunicación a Clientes Morosos	124
4.4.2	Proceso: Generación diaria de archivos de pagos.....	132
4.4.3	Proceso: Novedades de los reportes a las centrales de riesgo ..	136
4.4.4	Proceso: Marcación de reclamos en las centrales de riesgo	146
5	Arquitectura de servicios	149
5.2	Objetivos de la arquitectura de servicios	149
5.3	Portafolio de servicios.....	150

5.3.1	Servicios	150
5.3.2	Jerarquía de Servicios	152
5.4	Dependencias, composición y flujo de servicios	164
5.5	Requerimientos no funcionales de servicios	167
6	Arquitectura técnica.....	168
6.2	Propuesta de tecnologías soa	169
6.2.1	Tecnología Oracle.....	169
6.2.2	Tecnología IBM.....	170
6.2.3	Tecnología TIBCO	173
7	Conclusiones.....	175
8	Bibliografía	178

TABLAS

Tabla 1: Contexto del problema.....	25
Tabla 2: Producto obtenido del proyecto	27
Tabla 3: Involucrados a nivel corporativo.....	29
Tabla 4: Puntos de participación para los interesados.....	31
Tabla 5: Descripción de necesidades para el Principio de veracidad o calidad de los registros de datos.....	39
Tabla 6: Descripción de necesidades para el cumplimiento del principio de finalidad.	40
Tabla 7: Descripción de necesidades para cumplimiento del principio de seguridad.	41
Tabla 8: Descripción de necesidades para el cumplimiento el principio de confidencialidad.	42
Tabla 9: Descripción de necesidades para el cumplimiento del numeral 2.2 del Art. 6 de la Ley Habeas Data.	43
Tabla 10: Descripción de necesidades para el cumplimiento del numeral 3.3 de la Ley Habeas Data.	43
Tabla 11: Descripción de necesidades para el cumplimiento de los deberes de las fuentes de información.....	44

Tabla 12: Descripción de necesidades para el reporte de datos a las centrales de riesgo.	45
Tabla 13: Descripción de necesidades para la rectificación de información.	45
Tabla 14: Descripción de necesidades para la rectificación de información.	46
Tabla 15: Descripción de necesidades para certificación semestral de información.	46
Tabla 16: Descripción de necesidades para cumplir el principio de favorecimiento.	47
Tabla 17: Descripción de necesidades para cumplir requisitos especiales para fuentes.	47
Tabla 18: Descripción de necesidades para cumplir con el contenido de la información.	49
Tabla 19: Descripción de necesidades para darle acceso a la información a los usuarios.	49
Tabla 20: Descripción de necesidades para implementar mecanismos de PQRS.	50
Tabla 21: Descripción de necesidades para no incurrir en sanciones.	51
Tabla 22: Procesos misionales base de organización financiera.....	68
Tabla 23: Matriz de responsabilidades	115
Tabla 24: Roles requeridos para ejecución de procesos	116
Tabla 25: Tabla de atributos Registrar parámetros comunicado Habeas Data en SARC.....	124

Tabla 26: Tabla de atributos registrar población de clientes y/o codeudores morosos	124
Tabla 27: Tabla de atributos para la generación de población de clientes y/o codeudores morosos	127
Tabla 28: Tabla de atributos para modificar registros al archivo de clientes y/o codeudores morosos	131
Tabla 29: Tabla de atributos generar archivos de pagos e incumplidos	132
Tabla 30: Tabla de atributos para parametrizar claves para cifrar archivos en SARC	136
Tabla 31: Tabla de atributos para actualizar obligaciones de los reportes generados a las centrales de riesgo	136
Tabla 32: Tabla de atributos para la consulta de reportes de las centrales de riesgo en SARC	137
Tabla 33: Tabla de atributos para la generación de archivo consolidado de reclamos	146
Tabla 34: Tabla de clasificación de servicios	154
Tabla 35: Flujo de mensajes entre servicios	159
Tabla 36: Dependencias entre servicios	164

ILUSTRACIONES

Ilustración 1: Distribución de interesados a nivel proyecto	30
Ilustración 2: Componentes de SARC	35
Ilustración 3: Diagrama de contexto de la Ley Habeas Data en el Sector Financiero	65
Ilustración 4: Procesos misionales.....	68
Ilustración 5: Diagrama de Administración de la Información	73
Ilustración 6: Proceso de Circulación de la Información.	74
Ilustración 7: Proceso de consultas y reclamaciones.....	75
Ilustración 8: Proceso de comunicación a clientes morosos.....	76
Ilustración 9: Proceso de generación diaria de proceso de pago.....	89
Ilustración 10: Proceso de reporte de novedades a centrales de riesgo.....	95
Ilustración 11: Proceso de marcación de reclamos a centrales de riesgo	104
Ilustración 12: Proceso de disposición de información	119
Ilustración 13: Proceso de reporte de novedades.....	120

Ilustración 14: Macroproceso discernimiento PQRS.....	122
Ilustración 15: Componentes de Oracle SOA Suite	169
Ilustración 16: Arquitectura de referencia SOA de IBM	172
Ilustración 17: Arquitectura SOA de Tibco	173

1 INTRODUCCIÓN

Cada día aumenta la cantidad de información personal que es almacenada en bases de datos de diferentes entidades, tanto públicas como privadas, para fines comerciales, legales y financieros, entre otros. Ante tantas fuentes de información y las facilidades tecnológicas para intercambiar datos crece la posibilidad que dichos datos sean utilizados para fines diferentes de su destinación original o estén incompletos, errados o desactualizados, afectando así ostensiblemente el desarrollo social, comercial y privado de las personas lo cual se traduce en una vulnerabilidad de su derecho a la intimidad y al buen nombre.

Para regular el tratamiento que las empresas realizan con la información personal surgen varias leyes para la protección de datos como la ley 1266 de 2008 habeas data que refuerza el derecho a la privacidad contemplado en la constitución política de 1991 [19].

Dada la obligatoriedad del cumplimiento de dichas leyes en el sector empresarial, específicamente en el sector financiero, surge la necesidad de implementar soluciones tecnológicas que satisfagan los requerimientos legales en protección de información. Pero estas soluciones no son ni pueden ser componentes aislados de la plataforma tecnología de los sistemas de información existentes y deben articularse eficientemente al modelo arquitectónico ya definido.

Por la necesidad apremiante de implementar estas soluciones, puesto que las entidades reguladoras dan fechas específicas para el cumplimiento de sus disposiciones, las empresas se ven abocadas a implantar soluciones sin la adecuada metodología, sin políticas, estándares y ni procedimientos previos. Así se desarrollan aplicaciones e integraciones que cumplen puntualmente con lo que se requiere a nivel de seguridad pero que por lo general presentan rápidamente obsolescencia, sin posibilidad de escalamiento y están desarticuladas.

Por lo anterior, se propone el desarrollo de un modelo arquitectónico basado en los enfoques de los frameworks de Arquitectura Empresarial más reconocido de la industria como TOGAF [1] y Extreme Architecture Framework (XAF) [3]. Así, se establece una metodología robusta, flexible y de rápida adecuación para la implantación de la normatividad vigente en cuanto a la protección y seguridad de la información personal.

2 VISIÓN DEL PROYECTO

2.1 POSICIONAMIENTO DEL PROYECTO

2.1.1 Definición del problema.

Tabla 1: Contexto del problema

Problema es:	Las entidades financieras deben garantizar que la gestión de la información publicada en los bancos de datos de las centrales de riesgo Cifin y Datacrédito, se realice según lo dispuesto en la Ley 1266 de Habeas Data emitida el 31 de diciembre de 2008, cuyas sanciones por incumplimiento empiezan a regir a partir del 1 de Julio de 2009.
Afecta a:	Entidades Financieras. Específicamente las direcciones o departamentos de: <ul style="list-style-type: none"> • Riesgo, Crédito y Contraloría • Organización y Métodos • Tecnología
El impacto es:	Dentro del marco de seguridad exigido por la Ley Habeas Data, la entidad financiera impactada debe ajustar sus procedimientos de manera que pueda garantizar: <ul style="list-style-type: none"> • La correcta generación del reporte a centrales de riesgo. • Validación y corrección de inconsistencias enviadas por las centrales de riesgo. • Atención a los reclamos presentados por los clientes dentro del tiempo limite establecido por la ley. • Informar a los clientes que tiene sus obligaciones vencidas que serán reportadas a las centrales de riesgo. • Administrar correctamente las claves y consultas que se realizan a las centrales de riesgo
La solución satisfactoria	Implementar un marco de referencia de arquitectura orientada a servicios que permita a las entidades

sería:	financieras una implementación ágil de la ley Habeas Data para la protección de datos personales de los clientes.
--------	---

2.1.2 Objetivos del proyecto

- **Objetivo General.** Diseñar una arquitectura de referencia que permita a las entidades financieras colombianas implementar, según el paradigma de orientación a servicios, los requerimientos tecnológicos que genera el cumplimiento de la Ley 1266 de Habeas Data emitida el 31 de diciembre de 2008.
- **Objetivos Específicos**
 - Identificar a partir de la Ley 1266 de Habeas Data los requerimientos con alto impacto tecnológico en las entidades financieras colombianas.
 - Diseñar una arquitectura de negocio con procesos genéricos que correspondan a los requerimientos tecnológicos derivados de la implementación de la ley Habeas Data.
 - Definir el primer nivel de la arquitectura de información que debe responder el negocio para la ejecución de los procesos que dan cumplimiento a la ley Habeas Data.
 - Generar un esquema de servicios candidatos para ser implementados en la infraestructura tecnológica de una entidad financiera, basándose en el paradigma de Arquitectura Orientada a Servicios definida por RUP/SOMA [11].
 - Identificar las plataformas de tecnología SOA más influyentes del mercado para encaminar a las entidades financieras que requieren seleccionar la infraestructura que soporte la creación, despliegue y administración de servicios.

2.1.3 Definición del posicionamiento del producto

Tabla 2: Producto obtenido del proyecto

Objetivo del cliente:	Establecer una metodología que facilite el análisis del negocio, la información, las aplicaciones (integraciones) y la plataforma técnica de cualquier entidad financiera que propenda a estructurar una Arquitectura Orientada a Servicios para implementación de la protección de datos planteada por la ley Habeas Data.
Necesidad u oportunidad:	<p>Dar cumplimiento a la Ley de Habeas Data cuyos puntos principales son:</p> <p>Garantizar que la información reportada a las centrales de riesgo sea veraz, completa, exacta, actualizada, comprobable y comprensible.</p> <p>Tener los mecanismos ágiles y eficaces para la corrección de la información inconsistente antes y después de enviar los reportes a las centrales de riesgo.</p> <p>Atender los reclamos dentro del plazo que establece la ley.</p> <p>Informar a los clientes que tienen sus obligaciones vencidas, por las cuales serán reportados como morosos a las centrales de riesgo.</p> <p>Marcar y desmarcar, en los bancos de datos de las centrales de riesgo, los clientes que tienen un proceso de reclamación.</p> <p>La entidad financiera debe contar con la autorización del 100% de los clientes para ser reportados y consultados en las centrales de riesgo.</p> <p>La correcta administración de las claves y consultas que se realizan a las centrales de riesgo.</p> <p>Aplicar los principios de seguridad exigidos por la ley de Habeas Data.</p> <p>Algunos productos a ajustar son: Cartera Total, Endeudamiento Global, Tarjeta de Crédito Visa y Master Card y Cuentas Corrientes.</p>

<p>Producto:</p>	<p>Marco de referencia de Arquitectura Orientada a Servicios basado en TOGAF, XAF y RUP-SOMA para la implementación de la Ley Habeas Data, que permita una rápida adaptación de los procesos de la organización y tenga el mínimo impacto sobre la infraestructura tecnológica actual de la entidad financiera.</p> <p>El marco de referencia, contempla diferentes vistas del problema:</p> <p>Arquitectura de negocio. Implementación de las estrategias de negocio y la definición de procesos.</p> <p>Arquitectura de información. Define la información que la organización requiere para ejecutar los procesos.</p> <p>Arquitectura de aplicación. Servicios que soportan los procesos de negocio y alineación con la organización.</p> <p>Arquitectura tecnológica. Representa la tecnología, infraestructura y ambiente requerido por las aplicaciones que soportan los procesos de negocio.</p>
<p>Ventajas:</p>	<p>Actualmente, las organizaciones colombianas en general se encuentran incursionando en conceptos de Arquitectura Empresarial y desarrollos SOA, por lo cual cuando se enfrentan a una iniciativa como la adaptación de la organización para el cumplimiento de una norma, la práctica más común es realizar una actualización de sistemas de información sin evaluar las necesidades e impacto de los cambios dentro de la organización. Con este proyecto, es posible que una organización del sector financiero pueda implementar la ley Habeas Data, a partir de una visión de Arquitectura Empresarial, sin que sea necesario ser un experto en el tema.</p>
<p>Diferenciador:</p>	<p>La estructura arquitectónica para la implementación de la Ley Habeas Data, se modela bajo el concepto MDA [17] (Model Driven Architecture) promovido por la OMG.</p> <p>El uso de MDA garantiza que la funcionalidad es definida en Modelos Independientes de la Plataforma (Platform-Independent Model o PIM) usando UML, permitiendo a cualquier organización adaptar fácilmente la estructura arquitectónica a su propia infraestructura tecnológica, generando modelos de plataforma específica (Platform-Specific Model o PSM). [17].</p>

2.2 DESCRIPCIÓN DE INTERESADOS

2.2.1 Sumario de involucrados a nivel corporativo.

Tabla 3: Involucrados a nivel corporativo

<i>Nombre</i>	<i>Descripción</i>	<i>Responsabilidades</i>
Unidad de Organización y Métodos	La Oficina de Organización y Métodos estructura, estandariza y mejora las actividades administrativas a cargo de las diferentes unidades que conforman una empresa, mediante la documentación de procesos y el análisis funcional correspondiente, en el marco de la misión, visión y objetivos estratégicos de la empresa.	Realizar GAP análisis [20] del proceso descrito dentro de la estructura arquitectónica propuesta y la entidad financiera particular que lo implanta. Definir procesos y procedimientos operativos requeridos para cumplir con la Ley Habeas Data.
Unidad de Riesgo, control y crédito	Implementar políticas, estrategias y procesos que permitan minimizar el riesgo al que se enfrenta la entidad financiera.	Asegurar la ejecución normal de las operaciones de la entidad financiera, salvaguardando su situación patrimonial, administrando integralmente el riesgo y velando por el cumplimiento de los estatutos generados por los organismos e control.
Unidad de atención al cliente (comercial)	Unidad para la administración de las relaciones comerciales con clientes o prospectos.	Establecer y administrar los canales a través de los cuales se puede mantener un contacto con los clientes y/o prospectos de cliente para soportar los procesos de preventa, venta, posventa y operación de los productos de un cliente.
Unidad de Tecnología	La unidad o la división de tecnología apoya la ejecución de los procesos de la organización.	Definición, instalación y mantenimiento de la infraestructura tecnológica óptima para el soporte de los procesos del negocio.

2.2.2 Sumario de involucrados a nivel de proyecto

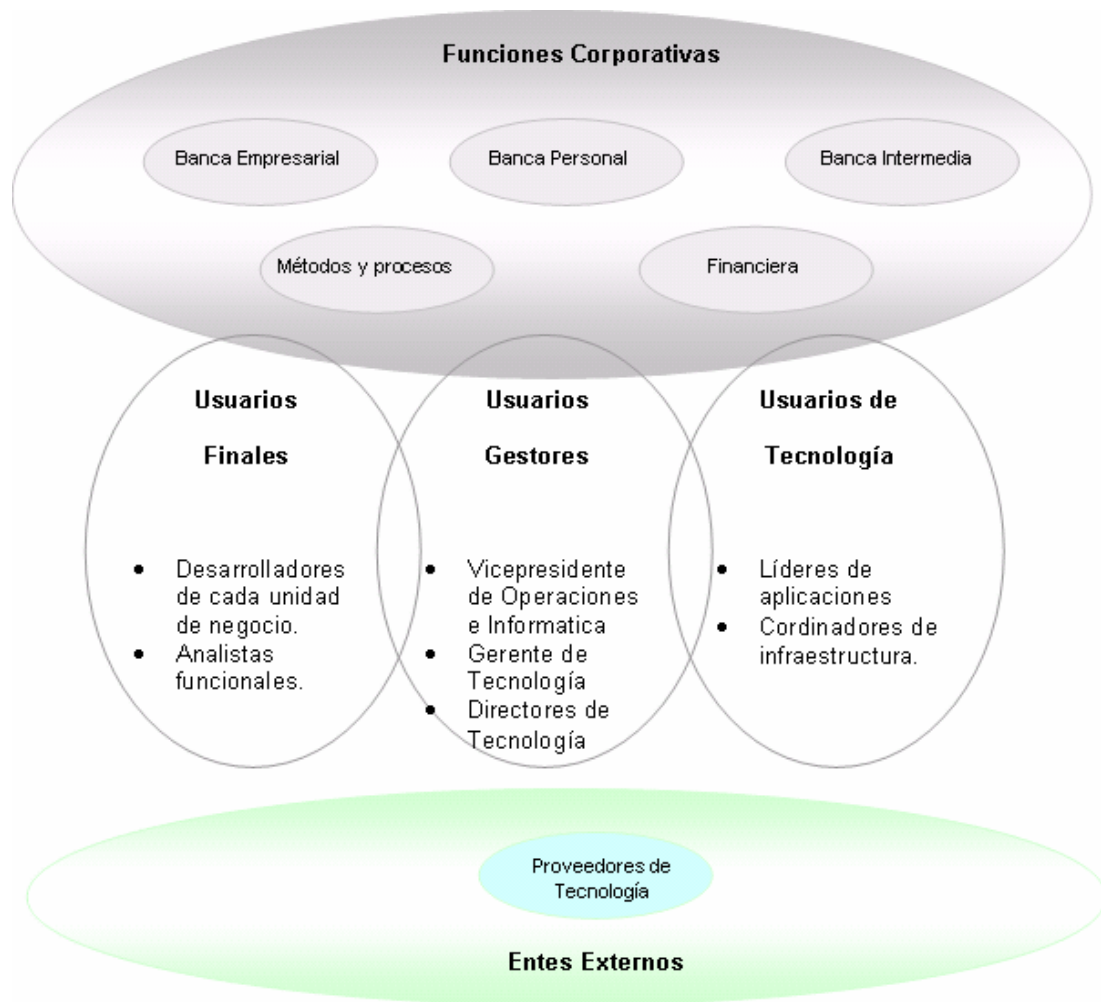


Ilustración 1: Distribución de interesados a nivel proyecto

Tabla 4: Puntos de participación para los interesados

<i>INTERESADOS</i>	<i>PUNTOS DE PARTICIPACIÓN</i>	<i>NECESIDAD</i>	<i>PUNTOS DE VISTA</i>
Gerente Corporativo	Este grupo de interesados, se interesa en tomar las decisiones de alto nivel, las metas y objetivos de la organización, y como son trasladados dentro de un proceso y la arquitectura de IT para avanzar el negocio	Mantener la Satisfacción	Diagrama Footprint del Negocio ¹ . [21].
CIO (Gerente de Tecnología Gerente de Procesos y Proyectos)	Este Grupo está interesado en las funciones y procesos de alto nivel de la organización, y de como sus aplicaciones principales de IT soporten estos procesos.	Miembros Claves	Organización, actores, localización, metas, objetivos y el modelo de servicio.
Directores de TI	Este grupo está interesado en que las iniciativas de cambio, se entreguen en el tiempo y presupuesto acordado y redunden en el beneficio de la organización.	Mantener Informado	Requerimientos de Arquitectura Principios de Arquitectura Visión de Arquitectura Descomposición Funcional Vista de localización de usuarios de aplicaciones

¹ TOGAF [REF21] define el diagrama footprint del negocio como la herramienta que permite describir “el enlace entre los objetivos del negocio, las unidades organizacionales, las funciones del negocio, y servicios, mapeando estas funciones a los componentes técnicos mostrando así la capacidad requerida. Provee una trazabilidad clara entre los componentes técnicos y el objetivo del negocio que este satisface, mientras también demuestra la propiedad de los servicios identificados”.

Líderes de aplicaciones y coordinadores de proyectos	Este grupo de interesados se encarga de especificar el diseño de los productos de tecnología a fin de satisfacer las necesidades de los proyectos y cumplir con la visión de arquitectura de la solución.	Miembros Claves	Vista de Ingeniería de Software Vista de Descomposición de Plataforma Procesos del sistema Vista de Realización Aplicación - Vista de Datos Vista de costos de migración de aplicaciones
Operadores de Infraestructura de TI	El grupo de interesados de infraestructura se ubican básicamente en lo concerniente con la localización, modificación, reusabilidad y habilitación de todos los componentes que integran la plataforma tecnológica para su óptimo comportamiento.	Miembros Claves	Vista de descomposición de plataformas Vista de estándares Vista de Administración Empresarial Vista de Hardware y Redes Vista de procesamiento Vista de Ambientes y Localización de componentes
Analista Funcional (Diferentes bancas)	Este grupo elaborará las plantillas de requerimientos para las iniciativas de cambio, basándose en la experiencia e interacción de los expertos del dominio con los usuarios finales de la organización.	Miembros Claves	Flujo de Procesos Casos de Uso Servicios e Información de Eventos Descomposición Funcional Aplicaciones - Vista de integración de aplicaciones
Analista Desarrollo (Diferentes bancas)	En este grupo se ubica: El enfoque de desarrollo, la modularidad de software y el reutilización, Migración e interoperabilidad.	Miembros Claves	Vista de ejecución del sistema. Vista de Datos Vista de Costo de migración de aplicaciones Vista de ingeniería

			de software Vista de componentes del sistema Vista de Distribución de Software.
--	--	--	---

2.2.1 Ambiente de usuario. La estructura arquitectónica para la implementación del Habeas Data, requiere que la empresa financiera que lo adopte cuente con: una plataforma tecnológica SOA, implantación de un Sistema de Administración de Riesgo Crediticio, Sistema para el manejo de PQRS y Sistemas financieros y contables para la administración de Tarjetas de Crédito y demás productos ofrecidos por la entidad que impliquen generar una obligación para el cliente.

- **Infraestructura SOA.** Una tecnología para el soporte de SOA, se basa en los siguientes conceptos:
 - Procesos de negocio. Modelamiento de procesos de negocio basado en la metodología de BPM.
 - Arquitectura de datos. Modelamiento en XSD (XML Schema Definition) [22] y mapeo de datos usando XSL (XSL Transformations) [23], CSV (comma-separated values files) [24], Copybook [25], entre otros.
 - Mapeo de Interfaces.
 - Procesamiento de procesos de negocio. Desarrollo de procesos de negocio siguiendo el estandar de BPEL [26].
 - Integración basada en Web Services.
 - Bus de Servicio Empresarial (ESB) [9]. Plataforma de enrutamiento de transacciones bajo el paradigma de orientación a servicios.
 - Motor de Reglas de Negocio. [16].
 - Monitoreo de procesos. Gestión de indicadores de desempeño (Key Performance Indicator - KPI) [28], Tableros de Control (Dashboard) [27].
 - Adaptadores. Servicios de infraestructura que ofrecen conectividad a sistemas legados. [29].
 - SOA testing (funcionalidad y desempeño) [30]. Para servicios y procesos de negocio.
 - Registro de Servicios (UDDI). Modelo de Datos, WSDL, versiones. [31].

- Governance (Gobernabilidad) [13]. Administración de cambios, control de versiones, soporte y gestión de la calidad.

Actualmente, existen variadas opciones para la implantación de una infraestructura SOA. Existen múltiples y variadas plataformas que soportan el paradigma de orientación a servicios más; una de las más reconocidas del mercado son: Oracle SOA Suite [32], Oracle BEA AquaLogic [33], IBM WebSphere Software Suite [34], TIBCO [35], Microsoft BizTalkServer [36], SUN Java CAPS [37].

- Sistema de Administración de Riesgo Crediticio (SARC). La Superintendencia Financiera de Colombia, mediante el Capítulo II de la Circular Básica Contable y Financiera [6], establece los lineamientos generales para la administración del riesgo crediticio en el portafolio de créditos de las entidades vigiladas financieras vigiladas. Se hace énfasis, entre otros aspectos, en la necesidad de: tener unas políticas claras y una estructura institucional adecuada para controlar y administrar el riesgo de crédito; desarrollar metodologías y bases de datos idóneas que permitan medir con una frecuencia adecuada las pérdidas esperadas derivadas del mismo; diseñar e implementar sistemas para minimizar dichas pérdidas en caso de incumplimiento de las contrapartes y desarrollar planes de contingencia para eventos catastróficos (SARC).

El sistema de administración del riesgo crediticio (SARC) en una entidad financiera debe contar al menos con los componentes básicos. [6].

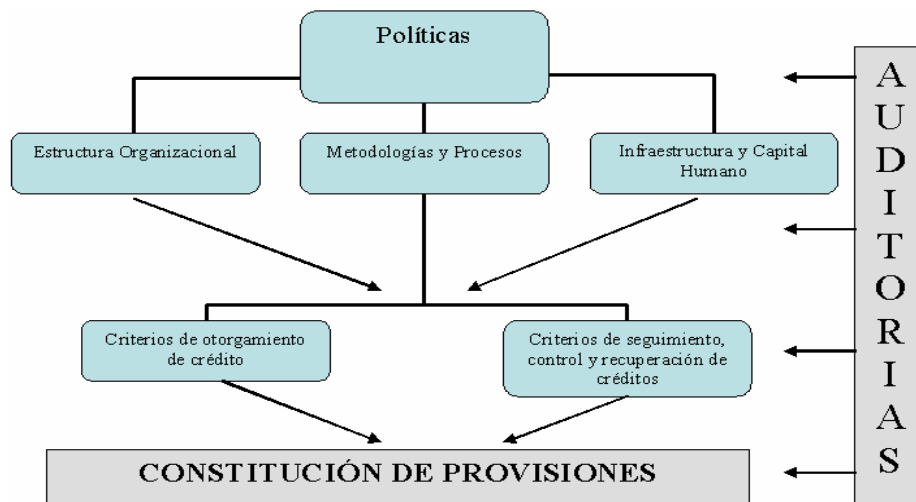


Ilustración 2: Componentes de SARC

El Sistema de administración de Riesgo Crediticio, permite proveer los indicadores y alertas para determinar los montos a desembolsar, detector de clientes incumplidos y generar la provisión para reportar a la Superfinanciera.

- Sistema o módulo para la administración de Peticiones, Quejas, Reclamos y Solicitudes (PQRS): Hace referencia a un sistema de información capaz de gestionar y administrar eficientemente las Peticiones, Quejas y Reclamos que radiquen los clientes de la entidad financiera. Las funcionalidades básicas que debe soportar el módulo PQRS son:
 - Registro y atención de usuarios a través de los diferentes canales que la organización hubiese dispuesto para ello (correo electrónico, fax, telefonía, cartas radicadas, entre otros).
 - Generación y seguimiento de solicitudes de PQRS, asignando al cliente un Ticket para la identificación del caso hasta su solución.
 - Permite seguimiento y escalamiento de solicitudes PQRS.
 - Estadísticos e indicadores de gestión y atención a casos.

- Sistemas financieros y contables. Básicamente hace referencia al sistema o sistemas de información, que administran los créditos de las diferentes bancas que maneje la entidad financiera.

La aplicación debe soportar el servicio de creación del crédito con todas sus características dependiendo de la línea y clase de cartera. A la vez que genera administración de las garantías, deudores, tasas de crédito, desembolso de crédito, seguimiento del pago de crédito y facilita el manejo de todo el ciclo de vida del crédito.

2.3 DESCRIPCIÓN DEL PRODUCTO

2.3.1 Perspectiva del producto. El proyecto genera una definición de una visión estándar para la implantación de la Ley Habeas Data, confluyendo en los lineamientos para las entidades financieras.

Establecer una metodología que facilite el análisis del negocio, la información, las aplicaciones y la plataforma técnica de cualquier entidad financiera que propenda a estructurar, bajo la conceptualización de una arquitectura empresarial basada en servicios, un modelo de protección de datos siguiendo los lineamientos de la Ley 1266 de Habeas Data.

- **Metodología.** La estructura arquitectónica se definirá siguiendo el Framework de Arquitectura Extrema (Extrem Architecture Framework – XAF) [3] que permite a partir de perspectiva minimalista cubrir ágilmente todos los dominios de arquitectura empresarial definidos desde los frameworks de Zachman y Togaf.

La arquitectura empresarial se descompone en los siguientes dominios de arquitectura:

- Arquitectura de Negocio o Actividad. Describe las actividades de negocio empresariales de alto nivel y flujos de trabajo.
- Arquitectura de Información. Describe la información requerida para soportar las actividades del negocio descritas en la Arquitectura de Actividad.

- Arquitectura de Software. Describe el software que es requerido para soportar las arquitecturas de actividad e información.
- Arquitectura Tecnológica. Describe el ambiente técnico en el cual el software se ejecuta.
- **Modelamiento arquitectónico.** El modelo de referencia técnico para la implementación de la Ley Habeas Data, incluirá desde cada una de las vistas o dominios de arquitectura, los procesos y servicios genéricos que deben estar disponibles en la organización, agrupándolos en clasificaciones lógicas en lugar de identificar productos específicos o soluciones, para que el modelo de referencia pueda ser portable, interoperable y reutilizable en diferentes organizaciones del sector financiero colombiano. Para lograr ese cometido, el modelamiento de la arquitectura se estructurará siguiendo los lineamientos definidos por la metodología MDA (Model Driven Architecture), la cual es propuesta y patrocinada por la organización Object Management Group (OMG).

La metodología MDA permite especificar un sistema independiente de la plataforma (Platform Independent Model - PIM) de manera que la organización que seleccione la Estructura Arquitectónica resultante de este proyecto, puede seleccionar la plataforma sobre la cual opera su organización y transformar la especificación independiente de la plataforma para una la plataforma escogida; es decir transformar el PIM a un PSM (Platform Specific Model).

- **Modelado de Servicios.** El modelo de servicio es una abstracción de los servicios de TI de una empresa y dan soporte al desarrollo de una o más soluciones orientadas a servicios. Se utiliza para concebir y documentar el diseño de los servicios de software. Se trata de un producto de trabajo compuesto completo que engloba todos los servicios, proveedores, especificaciones, particiones, mensajes, colaboraciones y relaciones entre ellos. Es necesario para identificar servicios candidatos y capturar decisiones sobre qué servicios serán realmente expuestos. [6].

IBM, para el desarrollo de servicios empresariales, implementó el método RUP - SOMA, el cual guiará el modelado de servicios para el proyecto.

2.3.2 Supuestos y dependencias. El Proyecto se enmarcará en los procesos que involucra la implementación de la Ley Habeas Data cuyo impacto en la organización del sector financiero se mide a nivel operativo y de infraestructura tecnológica dependiente de los sistemas de Administración de Riesgo Crediticio (SARC), Atención de PQRS y Core Contable y Financiero; es decir que los procesos 100% operativos de las oficinas o áreas relacionadas con las autorizaciones de los clientes para la consulta y reporte a las centrales de riesgos se encuentran excluidos del alcance del proyecto.

La estructura resultante de la ejecución del proyecto, se desarrolla siguiendo un paradigma de arquitectura empresarial orientada a servicios, lo que supone que la empresa u organización que desee seguir dicha estructura debe contar con una infraestructura que soporte el patrón ESB (Enterprise Service Bus) para la implantación de servicios.

2.3.3 Necesidades y características. La ley Habeas Data, define unos principios, deberes y derechos fundamentales para la protección de los datos confidenciales de las personas naturales o jurídicas, los cuales enmarcan unas necesidades específicas para las entidades financieras que deben cumplir lo exigido por la ley.

- **Principio de veracidad o calidad de los datos.** “La información contenida en los Bancos de Datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error”. [7].

Descripción de los requerimientos basados en el punto A del artículo 4 de la ley Habeas Data.

Tabla 5: Descripción de necesidades para el Principio de veracidad o calidad de los registros de datos

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-001	Creación de clientes implementando en sus sistemas de información validaciones que permitan total confiabilidad de datos como NITs, tipos de identificación, creación de consorcios, fideicomisos, carnet diplomático, entre otros.	Técnico - procesos
RU-002	Correcta creación de codeudores y otros titulares de productos de cartera y cuenta corriente.	Técnico - procesos
RU-003	Preventiva los errores ocasionados por procesos o errores operativos, aplicación de pagos extemporáneos, prorrogas no aplicadas, entre otros.	Técnico
RU-004	Identificar los cambios de codeudor a deudor para los créditos de libranza y que a su vez estos sea reportados oportunamente a las centrales de riesgo.	Técnico - procesos
RU-005	Depurar información que se encuentra actualmente inconsistente y que hace referencia a los datos básicos y demás inconsistencias del reporte.	Operativo (Proceso)
RU-006	Modificar los registros no reportados informados por la CIFIN y que hacen parte de las inconsistencias.	Técnico - procesos
RU-007	Operación que permita la correcta eliminación de obligaciones de las bases por prescripción de la deuda u obligación de acuerdo a lo dispuesto por la Corte Constitucional (expediente PE-029, Artículo 8).	Operativo (Proceso)
RU-008	Validar si los pagares antiguos si poseen o no la autorización, y proceder a la eliminación en los reportes a centrales.	Operativo (Proceso)
RU-009	Filtrar los pagares que no poseen autorización para que sean marcados y no reportados a centrales de riesgo. (Ejemplo: pagares cartera castigada, cartera migrada, cuentas corrientes antiguas, tarjetas de crédito antiguas, entre otros).	Técnico - procesos
RU-010	Permitir la renovación de pagares muy antiguos y que posiblemente no contengan la autorización del cliente para efectos de reportes o consultas en centrales de riesgo.	Operativo (Proceso)

- **Principio de finalidad.** “La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto”. [7]

Descripción de los requerimientos basados en el punto B del artículo 4 de la ley Habeas Data.

Tabla 6: Descripción de necesidades para el cumplimiento del principio de finalidad.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-011	Validar y/o modificar el formato o texto de “Autorización del titular para consulta y reporte a centrales de riesgo”. Esta autorización debe contener una descripción amplia, en la cual se relacione la finalidad de la consulta, el destino y el objeto, entre otros. Esto debe ser incluido dentro del pagaré, contrato de vinculación y demás documentos relacionados.	Operativo (Proceso)
RU-012	Generar un procedimiento de Atención de Reclamos para cualquier persona natural o jurídica que no tenga relación comercial con la entidad financiera (no clientes), en el cual la gestión de la reclamación requiera generar una consulta a las centrales de riesgo.	Operativo (Proceso)
RU-013	Generar un procedimiento para la atención de reclamos realizados verbalmente para validar si es necesario realizar marcación en las centrales de riesgo y entregar al cliente un soporte del reclamo.	Técnico

- **Principio de Seguridad.** “La información que conforma los registros individuales constitutivos de los Bancos de Datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado”. [7].

Descripción de los requerimientos basados en el punto F del artículo 4 de la ley Habeas Data.

Tabla 7: Descripción de necesidades para cumplimiento del principio de seguridad.

No	Necesidad	Nivel de Impacto
RU-014*	Establecer mecanismos para garantizar la correcta y debida custodia de las consultas, garantizando la seguridad de los documentos, evitando la adulteración, pérdida o uso indebido de la misma.	Técnico - procesos
RU-015*	Generar un procedimiento de solicitud de claves para los usuarios de las consultas de CIFIN y Datacredito, a través de la asignación de perfiles, esto con el ánimo de controlar y dar cumplimiento a los procesos de seguridad y confidencialidad descritos en la ley.	Operativo (Proceso)
RU-016*	Generar un procedimiento para la administración de las claves de los funcionarios que salgan a vacaciones, cambien de puesto o se retiren de la entidad financiera.	Operativo (Proceso)
RU-017*	Toda información de tipo confidencial que se envíe por correo electrónico, debe enviarse cifrada, con el objetivo de garantizar el envío y transito seguro de la información y los datos de los clientes, los paz y salvos y demás información concerniente a Centrales de Riesgo. Esto desde y hacia las oficinas que solicitan aclaración del reporte, calificación y moras.	Técnico

***Nota:** Estos requerimientos también se encuentran contemplados en la circular 052 que ya se encuentra implementada por ley en todas las entidades financieras regulas por la Superintendencia Financiera de Colombia.

- **Principio de confidencialidad.** “Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo solo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma”. [7].

Descripción de los requerimientos basados en el punto G del artículo 4 de la ley Habeas Data.

Tabla 8: Descripción de necesidades para el cumplimiento el principio de confidencialidad.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-018	Establecer un mecanismo operativo que garantice la reserva de la información, incluso después de utilizarla para los fines determinados y aún finalizada la relación con la labor del funcionario, inclusive si éste es retirado de la entidad.	Operativo (Proceso)
RU-019	Generar un procedimiento que garantice el correcto uso de las claves (ej: para evitar consultas no autorizadas).	Operativo (Proceso)

- **Derechos de los titulares de la Información.** Los derechos de los titulares de la información, descritos en el artículo 6 de la Ley Habeas Data, garantiza la existencia de procedimientos adecuados para la gestión de notificaciones y reclamaciones de los clientes sobre la información reportada sobre ellos a las centrales de riesgo.

Tabla 9: Descripción de necesidades para el cumplimiento del numeral 2.2 del Art. 6 de la Ley Habeas Data.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-020	El sistema de peticiones, quejas, reclamos y solicitudes de la entidad financiera debe cumplir con las normas establecidas para la correcta atención de reclamos.	Operativo (Proceso de Atención de reclamos de la entidad)
RU-021	El registro de incidentes desde el sistema de peticiones, quejas, reclamos y solicitudes de la entidad financiera debe garantizar el registro y la oportunidad de la totalidad de reclamos dando cumplimiento a los requerimientos de la ley.	Operativo (Proceso de Atención de reclamos de la entidad)
RU-022	La entidad financiera debe contar con la estructura óptima para la atención de reclamos de manera que se garantice la oportunidad y calidad que exige la ley.	Operativo (Proceso de Atención de reclamos de la entidad)

Tabla 10: Descripción de necesidades para el cumplimiento del numeral 3.3 de la Ley Habeas Data.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-023	Definir un procedimiento de custodia y consulta de la autorización del cliente, para cuando éste solicite la existencia de la autorización.	Operativo (Proceso)

Nota: Los requerimientos descritos para los anteriores artículos deben estar contemplados y cubiertos por el módulo de Atención de Quejas y Reclamos del que dispone la entidad.

- **Deberes de las fuentes de información.** En el artículo 8 de la Ley Estatutaria 1266, Habeas Data, se describe las obligaciones que deben cumplir las fuentes de información, entendiéndose como fuente de información a la “persona, entidad u organización que recibe o conoce datos personales de los titulares de información, en virtud de alguna relación comercial o de servicio de cualquier otra índole” [7].

Tabla 11: Descripción de necesidades para el cumplimiento de los deberes de las fuentes de información.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-024	Garantizar que los reportes de Tarjeta de Crédito, Cuenta Corriente, Cartera Total, Endeudamiento Global, se generen con la calidad y veracidad de los datos contenidos. Para esto es necesario que en el momento de la generación de los reportes se implementen validaciones de información y un mecanismo que permita realizar las correcciones en este archivo antes de su envío, conservando registro de los cambios realizados al reporte por corrección.	Técnico - procesos
RU-025	Para la generación de los archivos de pago para centrales a través de la funcionalidad ‘Generación de pagos’ disponibles en el sistema SARC, es necesario que las aplicaciones fuentes generen los pagos y novedades con igual periodicidad a la requerida para los archivos de pagos para las centrales de riesgo, con el fin de garantizar archivos que contienen información completa y actualizada.	Técnico - procesos
RU-026	Implementar un mecanismo que permita corregir los archivos enviados a las centrales de riesgo, cuando estos son devueltos o rechazados por inconsistencias devueltas, conservando la historia de lo ocurrido.	Técnico - procesos
RU-027	Generar procedimientos de validación de la información reportada a las centrales de Riesgo de manera que se garantice que es completa, exacta y actualizada.	Técnico - procesos

El numeral 2 del artículo 8, de la Ley Habeas Data, define que las fuentes de información (para nuestro contexto, las fuentes de información son las entidades

financieras), deben “reportar de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado”[7]. Esto obliga a las entidades financieras a reportar a las centrales de riesgo (Cifin y Datacrédito) las novedades sobre el cumplimiento de las obligaciones financieras de sus clientes ó titulares de información; por lo cual, se describen las siguientes necesidades:

Tabla 12: Descripción de necesidades para el reporte de datos a las centrales de riesgo.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-028	Permitir la actualización oportuna, permanente y periódica de la información en las centrales de riesgo CIFIN y Datacredito. (Ejemplo: pagos diarios).	Técnico - procesos
RU-029	El proceso de generación de paz y salvos debe ser consistente a la información de la cartera vigente y vencida del área de cobranzas de la entidad financiera, a fin de agilizar el proceso de paz y salvos garantizando el oportuno reporte de novedades al operador.	Técnico - procesos

El numeral 3 del artículo 8, de la Ley Habeas Data, define que las entidades financieras, deben “rectificar la información cuando sea incorrecta e informar oportunamente a los operadores” [7]. El cumplimiento de este deber, obliga que las entidades financieras cuenten con mecanismos que permitan a validar la constancia y veracidad de la información por parte de sus clientes, para lo cual, se describen las siguientes necesidades:

Tabla 13: Descripción de necesidades para la rectificación de información.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-030	Establecer un mecanismo que permita a las áreas que prestan el servicio de atención a solicitudes, quejas y reclamos, resolverlos con la calidad, oportunidad y tiempo establecido por la ley. El mecanismo debe	Técnico - procesos

	permitir al funcionario de la entidad financiera consultar de manera consolidada en el SARC las obligaciones del cliente y su comportamiento histórico (valores, saldos, cupos, entre otros).	
--	---	--

El numeral 4 del artículo 8, de la Ley Habeas Data, define que las entidades financieras, deben “diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador” [7]. El cumplimiento de este deber, las entidades financieras tienen la necesidad de disponer con los canales necesarios para enviar información completa y veraz a las centrales de riesgo.

Tabla 14: Descripción de necesidades para la rectificación de información.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-031	Generar con información completa, confiable y actualizada los archivos de cartera total, cuenta corriente, endeudamiento global, tarjeta de crédito y cuentas corrientes para las centrales de riesgo Cifin y Datacrédito, para que sean encriptados y enviados de manera automática.	Técnico - procesos

El numeral 6 del artículo 8, de la Ley Habeas Data, define que las entidades financieras, deben “certificar semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad” por parte del titular de la información [7]. El cumplimiento de este deber, implica el siguiente requerimiento:

Tabla 15: Descripción de necesidades para certificación semestral de información.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-032	Definir un procedimiento para la emisión de la certificación semestral a los operadores sobre las autorizaciones brindadas por clientes a la entidad financiera con la que adquirieron algún producto o servicio de dicha entidad.	Operativo (proceso)

- **Principio de favorecimiento a una actividad de interés público.** El parágrafo 1 del artículo 10 de la ley Habeas Data establece que se sancionará a las entidades financieras que “nieguen una solicitud de crédito basados exclusivamente en el reporte de información negativa del solicitante” [7]. Por lo cual las entidades deben responder a la siguiente necesidad:

Tabla 16: Descripción de necesidades para cumplir el principio de favorecimiento.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-033	Diseñar un mecanismo que permita informar al cliente las razones por las cuales no se realizó aprobación de un crédito, incluyendo razones diferentes al reporte negativo ocasionado por la mora en centrales de riesgo.	Operativo (proceso)

- **Requisitos especiales para fuentes.** El artículo 12 de la Ley Habeas Data, dispone que las entidades financieras deberán actualizar mensualmente la información suministrada a las centrales de riesgo y titulares de información.

Tabla 17: Descripción de necesidades para cumplir requisitos especiales para fuentes.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-034	La entidad financiera debe emitir una comunicación para informar a los clientes que alguna de las obligaciones adquiridas con la entidad se encuentra en mora y que por ese motivo será reportado ante las centrales de riesgo. El mecanismo de comunicación debe ser lo suficientemente ágil para permitir que 20 días después de la emisión de la comunicación se pueda realizar el reporte a las centrales riesgo o atender la queja, reclamo o petición del cliente.	Técnico - Procesos

RU-035	El archivo de cartera total debe generar la información segmentada por clientes y obligaciones para reportarlo a las centrales de riesgo con su estado al día. De igual manera debe generarse otro archivo con la segmentación de las obligaciones en mora el cual debe generarse y enviarse a las centrales de riesgo 20 días después de entregada la comunicación al cliente.	Técnico - Procesos
RU-036	Los reportes enviados a las centrales de riesgo que se generen por concepto de cuenta corriente, cartera total, tarjeta de crédito y endeudamiento global, deben excluir registros de obligaciones que se encuentren por debajo de un valor o porcentaje determinado por la entidad, y sea inferior treinta días de mora. Lo anterior, debe realizarse garantizando que no se genere inconsistencias por no reportar obligaciones a las centrales de riesgo.	Técnico - Procesos
RU-037	Se debe establecer un mecanismo que permita realizar ajustes sobre las obligaciones que tienen inconsistencias detectadas a partir de algún tipo de reclamación presentada por el titular. Esta funcionalidad se integra con los requerimientos descritos para el Artículo 8 punto 1 de la Ley Habeas Data.	Técnico - Procesos
RU-038	El módulo de PQRS de la entidad financiera, debe permitir tipificar los reclamos de manera que se pueda identificar aquellos que fueron originados a raíz de la comunicación enviada al cliente para informarle del reporte a las centrales de riesgo por mora en obligaciones.	Técnico - Procesos
RU-039	Implementar un procedimiento que permita actualizar el pago para los clientes que presentaron mora a corte de mes, pero que realizaron pagos durante los 20 días posteriores del aviso generado al cliente sobre reporte a las entidades de riesgo.	Técnico - Procesos

- **Contenido de la información.** Según el artículo 14 de la Ley Habeas Data, las entidades financieras deben reportar a las centrales de riesgo información en la que se pueda identificar datos referentes al titular de la información.

Tabla 18: Descripción de necesidades para cumplir con el contenido de la información.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-040	Generar reporte negativo y positivo para enviar a centrales de riesgo. (Nota: Se encuentra pendiente por la Superintendencia Financiera de Colombia la definición de los campos que debe conformar el reporte a las centrales de Riesgo).	Técnico - Procesos
RU-041	Los reportes debe incluir información referente al cupo de las obligaciones. (Actualmente no se está reportando esta información a las centrales de riesgo).	Técnico - Procesos

- **Acceso a la información por parte de los usuarios.** Según lo dispuesto en el artículo 15 de la Ley estatutaria 1566, Habeas Data, los datos de información financiera contenidos en las Centrales de Riesgo deberán ser consultados por las áreas que requieran generar estudio de mercado y/o verificar los riesgos para continuar con una relación contractual. Para cumplir con lo descrito por la ley, las entidades financieras deben cubrir las siguientes necesidades:

Tabla 19: Descripción de necesidades para darle acceso a la información a los usuarios.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-042	Definir un procedimiento que garantice que el área de Recursos Humanos, Recursos Administrativos, Seguridad y las demás áreas que utilizan la consulta a	Operativo (Proceso)

	centrales como mecanismo de validación o vinculación contractual diferente al otorgamiento de crédito o análisis de riesgo posean la autorización de las personas consultadas.	
RU-043	Reportar la forma de pago de las obligaciones que se cancelaron a través de un proceso Jurídico o mandato de pago, para que con dicha información se pueda calcular la correcta permanencia de estas obligaciones.	Técnico - Procesos
RU-044	Reportar el estado de discusión judicial para los casos en que el cliente no se encuentra de acuerdo con el reporte de mora generado por la entidad financiera, por lo cual ha iniciado un procesos jurídicos por algunas de las partes.	Técnico - Procesos

- **Peticiones, consultas y reclamos.** El artículo 16 de la Ley Habeas Data, exige a las entidades financieras poner a disposición de los titulares de información los medios para registrar y procesar peticiones, consultas y reclamaciones sobre el contenido de su información financiera.

Tabla 20: Descripción de necesidades para implementar mecanismos de PQRS.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-045	Diseñar un mecanismo que permita marcar y desmarcar en el reporte a centrales de riesgo de una manera diaria y automática, las obligaciones sobre las cuales los clientes presenten un reclamo por escrito. Es necesario que el módulo de PQRS de la entidad financiera pueda generar un reporte de los reclamos radicados y que estos se crucen con el SARC, de tal manera que sea posible homologar y asignar un número de obligación correcto a reportar a centrales. La entidad financiera debe almacenar en su base de datos de clientes todas las obligaciones reportadas, incluyendo el total de la cartera castigada.	Técnico - Procesos
RU-046	Implementar un mecanismo para realizar el control efectivo de los tiempos establecidos para dar respuesta	Técnico -

	a los trámites de reclamación por parte de los titulares de la información dentro de los plazos establecidos por la ley de habeas data. Si para la respuesta se requiere utilizar las prorrogas definidas en la ley, es necesario que se genere una comunicación informando al interesado el motivo de la demora y la fecha en que será atendido. Se debe generar las alertas de vencimiento e indicadores que permita el proceso: tiempo en que el cliente presenta el requerimiento, se registra en el módulo de PQRS, se envía al área solucionadora, se atiende y se envía la respuesta al cliente.	Procesos
RU-047	Para los reclamos radicados a través de operador, es necesario controlar el tiempo de respuesta y los reclamos pendientes de respuesta por cada una de las áreas solucionadoras.	Técnico - Procesos

- **Sanciones.** Según el artículo 18 de la Ley Habeas Data, el incumplimiento de la ley por parte de las entidades reguladas genera sanciones y multas por parte de la Superintendencia Financiera de Colombia. Para no incurrir en ningún tipo de penalización, la entidad deberá suplir las necesidades descritas a continuación:

Tabla 21: Descripción de necesidades para no incurrir en sanciones.

<i>No</i>	<i>Necesidad</i>	<i>Nivel de Impacto</i>
RU-048	Todos los funcionarios de la entidad financiera, y principalmente aquellos cuyas funciones se encuentran relacionadas con procesamiento, reporte o consulta de información de los clientes en las centrales de riesgo, deben conocer el régimen sancionatorio que establece la ley y sus responsabilidades en cuanto la calidad y confidencialidad de los datos.	Operativo (procesos)

2.4 ATRIBUTOS DE CALIDAD

La arquitectura debe estar orientada por los siguientes atributos de calidad:

- Interoperable (Interoperability). “Capacidad de dos o más sistemas o componentes para intercambiar información y utilizar la información que se ha intercambiado” [8]. La Arquitectura modelada para la estructura de implantación de la Ley Habeas Data, debe diseñarse garantizando las necesidades de transformación de datos que requieren los servicios de mediación, de tal manera que la entidad financiera pueda definir los adaptadores con los que debería disponer su ESB, según la naturaleza de sus sistemas involucrados.
- Portable (Portability). “Facilidad con que un sistema o un componente puede ser transferido de un entorno de hardware o software a otro” [8]. La Arquitectura diseñada debe poder transformarse a cualquier infraestructura de software o hardware del que disponga la organización que desee implementarla, siempre y cuando su funcionalidad sea equivalente a la que requiere la implantación de la estructura arquitectónica planteada.

3 ARQUITECTURA DE NEGOCIO

3.1 REPRESENTACIÓN ARQUITECTÓNICA

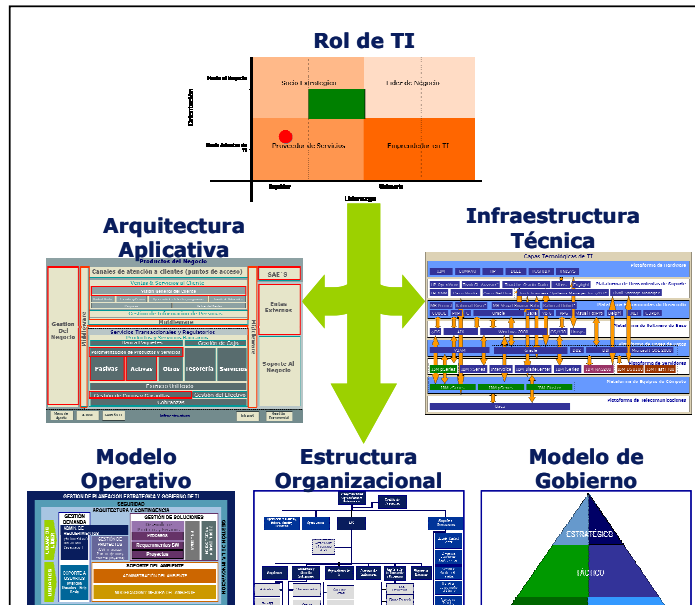
La representación de la arquitectura de negocio se efectuará haciendo uso de las siguientes vistas:

- Vista de Mercado. Permite identificar las influencias del mercado en la estrategia de la organización.
- Vista de Procesos de Negocio. Describe la forma en que se ejecutan los procesos misionales de la organización.
- Vista Organizacional. Da una visión general respecto a los roles que definidos en la organización, y que juegan algún papel en las definiciones dadas por la arquitectura para la ejecución de los procesos.
- Vista de Recursos Humanos. Visualiza los aspectos en los cuales las decisiones arquitectónicas afectan e involucran a las personas de la organización.

3.2 CONDUCTORES ARQUITECTÓNICOS

Esta sección describe los diferentes factores que influyen en las decisiones arquitectónicas descritas en este documento.

3.2.1 OBJETIVOS ARQUITECTÓNICOS



- Fortalecimiento interno de TI
 - Orientación de TI hacia el negocio
 - Alineación estratégica de TI
 - Mejora en la gestión y entrega de requerimientos
 - Montaje de las arquitecturas de TI

- Eficiencia de TI
 - Optimizar la eficiencia del área de TI hacia los requerimientos del negocio.
 - Planificación adecuada de costos e inversión en continuidad del negocio
 - Mejoramiento al sistema de gestión de seguridad
 - Mayor soporte de TI a las áreas administrativas y de soporte
 - Mayor oportunidad en el proceso de adquisiciones de TI

- Flexibilidad e integridad
 - Flexibilidad de los sistemas
 - Oportunidad de responder al mercado
 - Integridad, coherencia y oportunidad en toda la información del cliente
 - Bases para la integración de filiales

- **Motivación para generar implementación de soluciones desde la vista de metodología Arquitectura Orientada a Servicios**
 - Establecer una guía para facilitar la implementación de soluciones tecnológicas que responden al requerimiento del negocio, para el cumplimiento de estatutos que, como la Ley Habeas Data, generan un impacto directo algunos procesos de la entidad financiera.
 - Establecer una orientación para generar servicios de negocio reutilizables, centralizados y efectivos.
 - Crear, mantener y controlar lineamientos y estándares para propender el uso de las mejores prácticas del área de tecnología.

3.3 RESTRICCIONES ARQUITECTÓNICAS

3.3.1 Principios Empresariales.

<i>PRINCIPIO</i>	Alineación de la tecnología para alcanzar los objetivos de negocio.
<i>Justificación</i>	En aras de satisfacer las expectativas de crecimiento de la entidad financiera que requiere la implementación de la Ley Habeas Data, es un reto para el Área de Arquitectura gestionar eficientemente las estructuras tecnológicas asegurando el cumplimiento de los requerimientos del negocio. Por este motivo y con el propósito de apoyar la visión y las estrategias competitivas definidas en la organización, las Arquitecturas de TI serán la línea base para optimizar los procesos, disminuir costos, aumentar la calidad y fortalecer la disponibilidad tecnológica.
<i>Implicaciones</i>	El Área de Arquitectura deberá proponer las mejores prácticas que se adapten a la situación real de la empresa, utilizando mecanismos de proyección que le permitan planificar y analizar todo el escenario de TI encontrando el equilibrio de costo/beneficio óptimo para la organización. Por lo tanto, deberá ofrecer estándares y herramientas que permitan diseñar, modelar, comunicar y documentar eficientemente

	la arquitectura tecnológica que soporta los procesos del Banco.
--	---

PRINCIPIO	Evaluar el costo / beneficio de las propuestas de inversión en TI
<i>Justificación</i>	Al momento de decidir una incorporación tecnológica es necesario no perder de vista las necesidades del negocio ya sea que sus inversiones estén relacionadas con el mantenimiento o con el crecimiento. El proceso de inversión requiere de una planificación detallada y la aprobación del proyecto de un comité compuesto por diferentes áreas de la organización en las cuales debe estar presente el área de arquitectura para evaluar que la inversión represente una optimización de la arquitectura tecnológica del Banco, responda a los requerimientos de la empresa y presente beneficios económicos y operativos.
<i>Implicaciones</i>	<p>Arquitectura debe plantear una revisión periódica de la estrategia del negocio sobre el tipo de inversiones a hacer en tecnología, lo cual permite hacer un balance de las operaciones y decisiones del área en pro del negocio, la arquitectura de los sistemas y las operaciones.</p> <p>La evaluación del costo / beneficio de una inversión debe relacionar la proyección del crecimiento del negocio, el aumento de la cantidad de clientes, la penetración de productos y la visión que se propone.</p> <p>Realizar seguimiento y evaluación del resultado de las inversiones en tecnología y responsabilizarse del costo / beneficio obtenido.</p>

3.3.2 Principios Tecnológicos.

PRINCIPIO	Mantener una constante actualización tecnológica para garantizar un nivel óptimo en la atención de servicios provistos por TI.
<i>Justificación</i>	El cambio tecnológico ocurre con gran rapidez, lo que tiene implicaciones importantes para el uso eficiente de los recursos, la competitividad del área de TI y la determinación de ventajas comparativas para el negocio. Por esta razón, en la entidad financiera se debe garantizar establecer esquemas que permitan mantener una

	vigencia tecnológica pertinente que garantice prestación de servicios que aproveche las ventajas brindadas por la industria de la computación.
<i>Implicaciones</i>	<p>Proponer mecanismos para la expansión de conocimiento, actualización del mercado de la tecnología y adaptación de los procesos a nuevas tendencias como actividad complementaria de las labores diarias del personal de TI.</p> <p>Uso de herramientas de fácil utilización como Wikis y Blogs para promulgar conocimiento sobre procesos de negocio, funcionalidades de tecnología existentes en la entidad financiera y captar ideas de innovación y mejoramiento por parte de los empleados.</p> <p>Promover iniciativas para la actualización de Arquitectura con el fin de proveer un servicio de alta calidad, aprovechar las ventajas de nuevas tecnologías y responder de manera más eficiente a los requerimientos del negocio.</p> <p>Para administrar el abanico de oportunidades que presenta el mercado de Tecnología de Información es necesario conocer el plan de la división. Esto implica conocer la arquitectura técnica y la estrategia interna. Por esto el área de Arquitectura tiene que hacer un continuo seguimiento a las tendencias del mercado, evaluar qué es lo que los competidores están utilizando y cuáles son las tecnologías más fiables para soluciones informáticas.</p>

<i>PRINCIPIO</i>	Centralizar los mecanismos de seguridad y trazabilidad a las transacciones.
<i>Justificación</i>	La trazabilidad y el acceso a las funcionalidades se manejan de manera independiente por cada aplicación lo que dificulta rastrear, reconstruir o establecer un proceso de negocio a través de los registros de auditoria generados por cada sistema, ya que estos se almacenan en diferentes repositorios de datos. Por este motivo, es necesario implantar un procedimiento único de acceso a las aplicaciones y procedimientos de seguridad que implanten una trazabilidad centralizada a los procesos del negocio, eliminando los problemas asociados a la inconsistencia de los procesos de auditoria.
<i>Implicaciones</i>	Es necesario estandarizar los mecanismos de seguridad para todas las aplicaciones de la entidad financiera de manera que se centralicen los registros de acceso y la trazabilidad, debe usarse un modelo simple de registro de transacciones que permita almacenar la información en un repositorio único, el cual deberá ser accesible para realizar procesos de auditoria sobre las operaciones del negocio.

3.2.1 Principios de Software.

<i>PRINCIPIO</i>	Las propuestas de desarrollo o actualización tecnológica deben considerar el mínimo impacto sobre la arquitectura.
<i>Justificación</i>	Los procesos de actualización a las estrategias de negocio no involucran el Área de Arquitectura para la toma de decisiones, motivo por el cual los ambientes tecnológicos han crecido bajo demanda y con poca planeación, no se implementan lineamientos a nivel empresarial para proyectos de tecnología con características similares, generando redundancia de los servicios de TI y aumentando los costos de mantenimiento debido a que las aplicaciones son implementadas aisladamente con tecnologías heterogéneas y sin aplicar estándares ni mejores prácticas de desarrollo.
<i>Implicaciones</i>	<p>Validar cualquier propuesta de actualización para la Arquitectura de las aplicaciones a la luz de los lineamientos, estándares establecidos y nuevas tecnologías que den beneficios tangibles al negocio.</p> <p>El Área de Arquitectura debe ser integrante activo en los comités estratégicos para que conozca las estrategias del negocio y sus objetivos relacionados y se pueda tomar decisiones que establezcan las bases para una implementación futura la cual contemple el dominio de negocios como un componente adicional de la arquitectura empresarial.</p>

<i>PRINCIPIO</i>	Consolidar aplicaciones que utilicen la misma tecnología para optimizar el uso de la plataforma.
<i>Justificación</i>	En la actualidad las entidades financieras cuenta con una gran diversidad de aplicaciones las cuales se encuentran implantadas independientemente, sin integrarse entre si, lo que dificulta el control de las plataformas, el establecimiento de estándares para la infraestructura de aplicaciones y desperdicia la capacidad de los recursos físicos disponibles. Por tal motivo es necesario propender a la consolidación de la plataforma tecnológica que soporta las aplicaciones del negocio de manera que se optimice la administración y

	escalabilidad de la infraestructura existente.
<i>Implicaciones</i>	<p>Considerar un esquema de consolidación de los ambientes de desarrollo y almacenamiento para las aplicaciones que tienen una plataforma operativa común.</p> <p>Estandarizar paulatinamente la arquitectura sobre la que operan y se comparten servicios tales como correo electrónico, archivos compartidos, servicios de impresión, servicios de trabajo en grupo, entre otros.</p>

<i>PRINCIPIO</i>	Asegurar la interoperabilidad de las aplicaciones usando mecanismos estándar de comunicación.
<i>Justificación</i>	Actualmente las aplicaciones utilizan métodos propietarios para interactuar, lo cual genera múltiples problemas al momento de migrar a tecnologías nuevas o a estándares de intercambio de información, debido a que es necesario desarrollar nuevamente los componentes que implementan este servicio al interior de cada aplicación. Por este motivo es necesario que la Arquitectura de las aplicaciones se base en estándares, sea flexible a cambios, económico, y que garantice la interoperatividad entre las aplicaciones.
<i>Implicaciones</i>	El desarrollo de interfaces deberá hacerse teniendo en cuenta estándares de comunicación, lo cual en ocasiones puede ocasionar demoras adicionales en el intercambio.

3.2.2 Principios de Información y Datos.

<i>PRINCIPIO</i>	Permitir un acceso eficiente y eficaz a la información
------------------	--

<i>Justificación</i>	<p>El responsable de la información debe permitir que sea accedida de manera eficiente, y en un tiempo aceptable para las tareas en las que es necesario consultarla.</p> <p>Para el almacenamiento de la información y para la designación de su responsable se debe tener en cuenta que debe estar disponible para una amplia variedad de posibles accesos, algunos de ellos requiriendo tiempos de respuesta excelente, y otros requiriendo acceso en cualquier momento del día.</p>
<i>Implicaciones</i>	<p>Los mecanismos disponibles para acceder a la información deben ser lo suficientemente adaptables para permitir que la información sea consultada en una amplia variedad de usuarios, cada uno con diferente mecanismo de acceso y diferente necesidad.</p> <p>Se deben establecer mecanismos que garanticen la seguridad de la información, de modo que la facilidad de acceso no constituya un riesgo para un uso debido de la información.</p>

<i>PRINCIPIO</i>	Debe existir un responsable por cada elemento de información
<i>Justificación</i>	<p>Toda la información de la empresa debe tener un responsable, sus responsabilidades son:</p> <p>Garantizar que la información sea acertada</p> <p>Garantizar el acceso oportuno a la información</p> <p>Debe ser la fuente de transacciones que actúan sobre la información</p> <p>Debe brindar las funciones de compensación y contabilidad para esta información</p> <p>Uno de los beneficios de la orientación a servicios en la Arquitectura de TI es la habilidad para compartir la información. A medida que la información es compartida entre más y más sistemas, múltiples copias de la información aparecen, y por tanto es necesario que todos los usuarios que necesitan la información confíen en una única fuente. La existencia de múltiples fuentes de información conlleva a la aparición de inconsistencias en la misma.</p>
<i>Implicaciones</i>	<p>Es esencial que el responsable de la información pueda proveer acceso seguro a ella y mantener la confidencialidad de información de manera que no pueda ser consultada por personas no autorizadas.</p> <p>Para determinar quién es el responsable de la información, se debe identificar la verdadera fuente de la misma y tenerla en cuenta en la</p>

	decisión. Aunque es posible que la fuente y el responsable sean diferentes, siempre deben estar claramente identificados.
--	---

<i>PRINCIPIO</i>	Seguridad de la información
<i>Justificación</i>	Las leyes y reglamentaciones vigentes exigen la salvaguardia de información amparada por la reserva bancaria y aquella clasificada como confidencial según las políticas internas. Por este motivo, el Banco con el objetivo de realizar el debido cumplimiento de los estatutos legales y prestar el servicio más confiable a sus clientes, debe adoptar medidas que garanticen la seguridad de la información considerando todos los canales de distribución, evitando su filtración y uso inadecuado.
<i>Implicaciones</i>	<p>La arquitectura implementada por TI debe diseñarse considerando establecer barreras de protección y medidas de seguridad, las cuales garanticen que las aplicaciones, los datos y la infraestructura tecnológica estarán aseguradas de accesos no autorizados, manipulación, alteración, sabotaje o divulgación de la información.</p> <p>Arquitectura debe implementar mecanismos de contingencia para la seguridad de la información, monitoreo del acceso a datos y análisis de riesgos.</p> <p>El área de Arquitectura debe realizar auditoria de las barreras de seguridad implementadas por TI para minimizar riesgos, cubrir los requerimientos de los estatutos legales vigentes y las políticas internas.</p>

3.2.3 Principios de arquitectura para el proyecto.

<i>PRINCIPIO</i>	Utilizar protocolos y formatos estándar en los intercambios, siempre y cuando estos no afecten la velocidad, seguridad y calidad en general del servicio.
<i>Justificación</i>	El uso de estándares de mensajería y formatos de archivos facilita la interoperabilidad entre las aplicaciones del Banco y las aplicaciones de

	<p>terceros, disminuye la cantidad de desarrollos a la medida.</p> <p>La amplia diversidad de formatos en las interfaces dificulta la integración de unas aplicaciones con otras, incurriendo en la necesidad de realizar desarrollos o buscar alternativas que propician el desorden.</p>
<i>Implicaciones</i>	<p>En algunos casos, los estándares tienen desventajas inherentes. Cuando asumir estos estándares implique alguna de las siguientes desventajas, y estas sean inaceptables, puede optarse por establecer formatos propios del Banco, previa validación con Arquitectura.</p> <p>El uso de algunos estándares, como los WebServices, aumentan la cantidad de procesamiento necesaria tanto en la parte que envía la información, como de la parte que la interpreta.</p> <p>El uso de algunos estándares, como los WebServices, aumentan la cantidad de información que viaja por la red. Esto se hace crítico cuando es necesario enviar información binaria o cuando es una interfaz utilizada con mucha frecuencia.</p>

<i>PRINCIPIO</i>	<p>En los casos en los que alto desempeño sea necesario, la Arquitectura deberá garantizar que sus componentes no añadan demoras en el tiempo de respuesta.</p>
<i>Justificación</i>	<p>Es necesario propender por el orden en los intercambios de información, y también es necesario cumplir con los requerimientos de desempeño de las interfaces. En ocasiones no será posible cumplir totalmente con ambas necesidades, y en estos casos Arquitectura deberá brindar una alternativa que permita cumplir con los requerimientos de desempeño, o establecer que no es posible lograr los niveles de desempeño deseados.</p>
<i>Implicaciones</i>	<p>Es posible que para cumplir con alguno de los requerimientos no funcionales deba pasarse por alto alguno de los lineamientos de Arquitectura, en este caso, la excepción deberá incorporarse a la Arquitectura, detallando las ocasiones en las que dicha excepción es aceptable.</p> <p>Téngase en cuenta que el volumen de información está ligado a los requerimientos de desempeño o requerimientos no-funcionales requeridos por los intercambios de información. De la misma manera dependerá de cómo se orquesten los procesos bancarios que se ejecutaran dentro de la plataforma para transacciones de captación y en el bus empresarial de servicios.</p>

PRINCIPIO	La aplicación responsable del cliente es el CRM.
Justificación	Cada entidad de negocio debe ser administrada por una única aplicación.
Implicaciones	<p>Debido a que la información del cliente es propiedad del CRM:</p> <p>Las aplicaciones que requieran información del cliente deberán solicitarla al CRM.</p> <p>CRM es el punto inicial donde deben crearse los clientes.</p> <p>Debe garantizarse que los clientes únicos del <i>frontend</i> de captaciones y el ESB permanezcan sincronizados. Esto significa que una modificación en cualquiera de los dos clientes únicos debe replicarse al otro mediante una notificación en línea, usando al ESB para su despacho.</p>

3.3 VISTA DE MERCADO

3.3.1 Marco de negocio. [10].

- **Gestión eficiente del riesgo.** En este entorno, la institución financiera debe mejorar los métodos de identificación, gestión y valoración de los riesgos añadidos del crédito y de operaciones.

Del mismo modo que una visión más global de sus clientes puede mejorar las ventas, según los analistas, también puede proporcionar una idea más precisa de su riesgo de crédito y de fraude y sugerir estrategias para mejorar las actividades de cobro y recobro.

- **Gestión de la información.** Las instituciones necesitan procesos de negocio totalmente integrados. Éstos requieren infraestructuras de sistemas que puedan centralizar la gestión de la información de toda la empresa e incorporar interfaces con fuentes de datos externas, al tiempo que se controla el gasto de su gestión. Asimismo, se contribuye a la automatización y estandarización de los procesos de negocio en diferentes líneas y unidades organizativas.

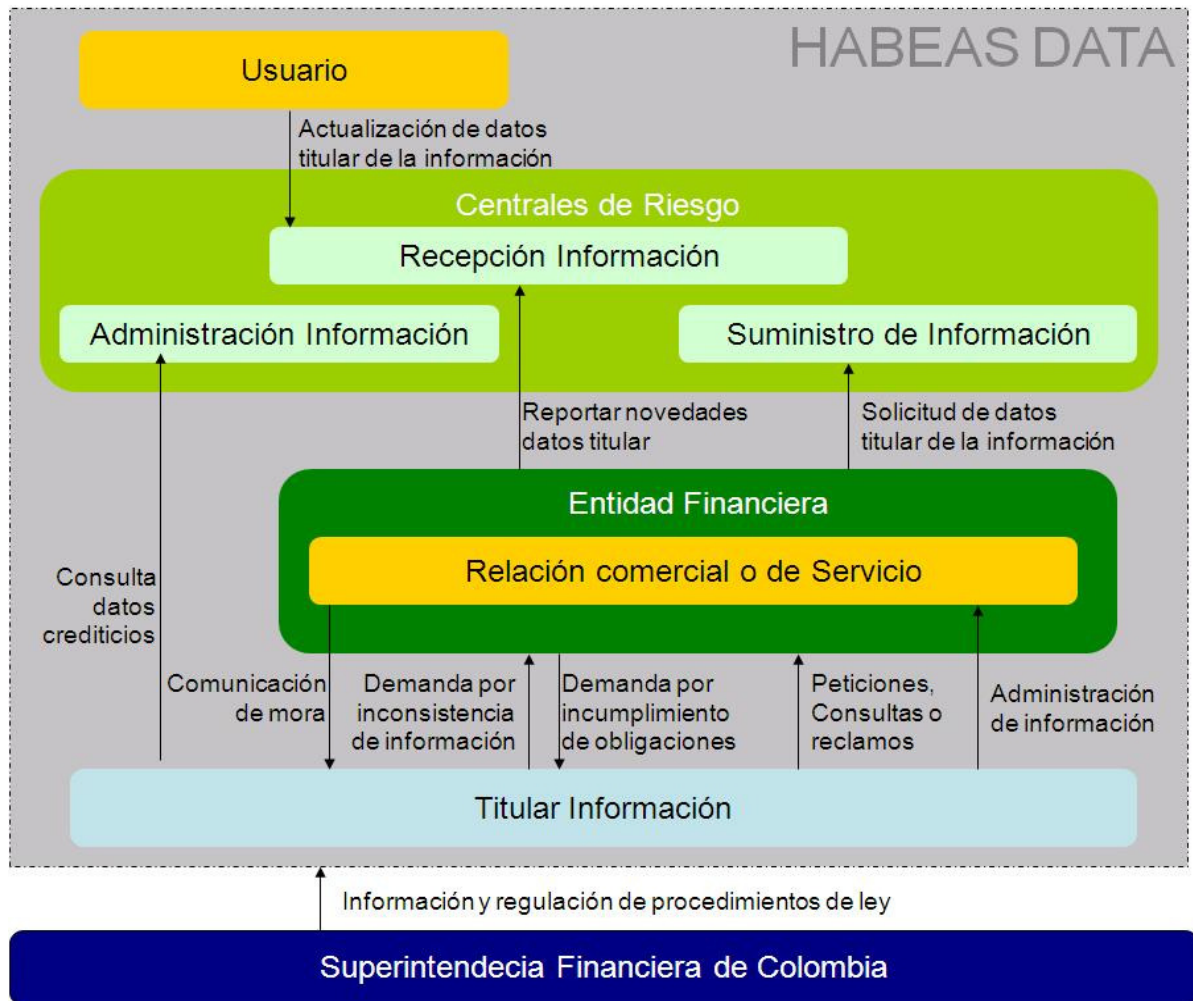
Para alcanzar estos objetivos, es necesaria una solución integrada, abierta, basada en componentes, que dé soporte a aplicaciones de terceros y que pueda adaptarse a su empresa.

- **Gestión de los clientes.** La arquitectura de aplicaciones debe orientarse a un enfoque abierto y basado en componentes para ofrecer la flexibilidad necesaria que permita ajustarse a las necesidades específicas del cliente, realizar análisis históricos del comportamiento de los clientes para que se generen estrategias de mercado que permitan fidelizar al cliente con la entidad.
- **Actualidad de los canales de distribución.** En la banca, la eficacia operativa se puede mejorar significativamente si se sustituyen las diferentes estrategias de aprovisionamiento por distintos canales por una única estrategia completamente integrada que utilice una arquitectura común.
- **Externalización de los procesos de negocio.** La arquitectura abierta de las soluciones debe permitir a la organización controlar sus procesos de negocio y, al mismo tiempo, externalizar determinadas funciones que forman parte de estos procesos.

Gracias a la infraestructura de las soluciones, la institución debería poder definir y controlar determinados procesos de negocio independientemente de su ubicación física o de las aplicaciones que los ejecuten.

3.3.2 Contexto de negocio

- Diagrama de contexto



[Fuente: Propia]

Ilustración 3: Diagrama de contexto de la Ley Habeas Data en el Sector Financiero

- **Descripción del contexto.** Para el cumplimiento de la ley Habeas Data en el sector financiero, es necesaria la interacción de las siguiente entidades para la ejecución de los procesos:

- Titular de la Información. Persona natural o jurídica referida en información privada, pública o semipública que repose en las centrales de riesgo o sea administrada por terceros con los hubiera establecido alguna relación comercial o jurídica.

El titular de la información por establecimiento de la Ley Habeas Data, tiene derechos constitucionales que le permiten:

- Ser informado cuando cualquier ente con el que hubiera establecido una relación comercial o de servicios va a reportarlo con deudor moroso a las Centrales de Riesgo.
 - Solicitar consulta, rectificación o actualización de su información crediticia cuando así lo requiera, esperando la respuesta oportuna de la entidad financiera.
 - Establecer demandas jurídicas por inconsistencia de su información.
- Usuario. El Usuario es una persona natural o jurídica que tiene acceso a información personal de titulares de la información; es decir que el Usuario puede ser la entidad financiera o un tercero que, por algún vínculo o interés comercial, conoce y genera información crediticia de un titular. Entre las funciones más importantes del usuario está el ser responsable de la veracidad y confiabilidad de los datos de los titulares de información, por lo cual debe generar actualizaciones periódicas a las Centrales de Riesgo.
 - Centrales de Riesgo. Las Centrales de Riesgo son una entidades que administran y almacenan información comercial de las personas naturales o jurídicas. En el sector financiero se debe reportar o solicitar información de las personas con las que se hubiera establecido una relación comercial a las entidades CIFIN y Datacrédito.
 - Entidad Financiera. "Entidad u organización que recibe o conoce los datos personales de los titulares de información en virtud de una relación comercial o de servicio de cualquier otra índole" [7].

La entidad financiera es responsable de garantizar y amparar la confiabilidad y confidencialidad de la información. Para ello debe ejecutar los siguientes procesos:

- Asegurar que el titular de la información autorice a la entidad financiera el conocimiento y manejo de sus datos.
 - Solicitar y actualizar periódicamente a las Centrales de Riesgo, la información comercial que se hubiera generado sobre sus clientes referente a procesos de cobro de cartera o actualización y rectificación de datos.
 - Disponer de los canales necesarios para que los titulares de información puedan solicitar consulta de información personal y radicar reclamaciones para actualización o rectificación de datos.
 - Generar un proceso que permita dar respuesta a las solicitudes o reclamaciones de un titular de información en un plazo inferior a 20 días.
 - Informar oportunamente a los clientes que tienen obligaciones incumplidas por saldos en mora que serán reportado a las centrales de riesgo. En caso que algún cliente se encuentre en desacuerdo con el reporte y notifique a la entidad financiera al respecto, la entidad debe informar a la Central de Riesgo que el cliente se encuentra en proceso de reclamación.
- Superintendencia Financiera de Colombia. La superintendencia Financiera de Colombia es un ente gubernamental adscrito al Ministerio de Hacienda y Crédito Público que se encarga de regular y supervisar que las entidades y grupos financieros ejecuten correctamente sus funciones según lo establecido por la ley.

3.4 VISTA DE PROCESO DE NEGOCIO

3.4.1 Procesos del negocio impactados por el proyecto



Ilustración 4: Procesos misionales

Tabla 22: Procesos misionales base de organización financiera

Procesos	Subprocesos	Objetivo del Proceso
I. DESARROLLO DE PRODUCTOS		
Diseño / Definición del Servicio	Diseño y definición del servicio	Definir e implementar productos y/o servicios con características y beneficios que satisfagan las necesidades de un segmento específico de clientes, generando valor agregado a la institución.
Gestión Comercial y Consecución del Cliente	Administración de Bancas	Cumplir con la estrategia comercial de la institución a través del contacto de clientes, usuarios y/o prospectos de banca masiva (persona natural y jurídica) y fidelización de los existentes.
	Banca Masiva	Cumplir con la estrategia de la institución a través del contacto de clientes de banca empresarial y fidelización de los existentes.
II. ADMINISTRACIÓN DE RIESGOS		

Vinculación del Cliente	Entrega de documentos de apertura o constitución de productos	Obtener, verificar y asegurar los documentos, requisitos e información que permitan cumplir con aspectos legales y normas establecidas para la vinculación y conocimiento de los clientes.
	Creación del cliente	Registrar con calidad, integridad, veracidad, suficiencia y completitud la información de los clientes en el sistema de la institución, para que ésta sea utilizada en futuras relaciones comerciales, consultas internas y responder a requerimientos de información exigidos por las entidades reguladoras.
	Apertura de los productos y/o servicios o constitución de productos	Identificar y asignar el producto al cliente en el sistema para su utilización en los diferentes procesos internos.
	Entrega de los productos y/o servicios	Registrar, asociar y entregar al cliente los documentos y medios necesarios para la utilización del producto y/o servicio.
	Plásticos	Facilitar la oportuna disponibilidad para la confirmación de la firma y condiciones del manejo de la cuenta para las diferentes transacciones realizadas por el cliente dando cumplimiento a las normas establecidas por la institución.
III. OPERACIONES		
Utilización del servicio por parte del Cliente	Depósitos	Facilitar al cliente utilizar la red de oficinas para que pueda realizar sus depósitos y cuenta con la disponibilidad de los recursos.

	Retiros	Brindar los canales y medios necesarios para que los clientes y/o usuarios puedan disponer de sus recursos.
	Embargos / desembargos	Registrar de forma oportuna, veraz y consistente una orden judicial o de organismo competente que ordene embargar o desembargar los depósitos que un cliente tenga.
	Cuadres	Verificar que los saldos de las cuentas de ahorro y cuentas corrientes y CDT's coincidan con los registros contables.
	Custodias	Verificar que la existencia física coincida con los registros contables.
	Generación de extractos	Generar oportunamente y con calidad un documento de validación que le permita al cliente verificar los movimientos de sus productos con la institución.
	Aprobación de tasas especiales	Atender los requerimientos de clientes, en cuanto la solicitud de Tasas preferenciales cumpliendo con las normas legales, las políticas y los controles internos.
	Liquidación de intereses y comisiones	Liquidar, contabilizar y pagar oportunamente a los clientes los rendimientos financieros producto de sus inversiones y depósitos.
	Compensación - Recibida	Recepcionar, verificar, procesar, y alistar los cheques devueltos impagados, para ser entregados a los clientes o reconsignados.
	Compensación - Enviada	Identificar y clasificar los cheques visados que presentaron causales de devolución para ser entregados a la Cámara de Compensación.
	Emisión de títulos físicos y Desmaterialización de Títulos	Minimizar el riesgo de la emisión de títulos, a través de la desmaterialización con entidades que prestan éste tipo de servicios.
	Estado de las Cuentas	Proteger los recursos de los clientes en los cambios de estado de las cuentas cumpliendo con las medidas de seguridad y la reglamentación interna y externa establecida.

IV. SERVICIO AL CLIENTE		
Mantenimiento del Servicio	Actualización de datos del cliente,	Permitir mantener actualizada la base de datos de los clientes y usuarios del Banco, permitiendo una buena gestión comercial y cumpliendo con la reglamentación de seguridad vigente.
	Quejas y reclamos	Dar respuesta completa y oportuna a las quejas que presentan los clientes a través de la Superintendencia Bancaria, Defensoría del Cliente Financiero, Otras Entidades Oficiales y por Derecho de Petición y efectuar la gestión de retroalimentación para mejorar los procesos en los que se originaron.
	Administración del efectivo	<p>Servicio Administración de Efectivo / Oficina Garantizar la oportunidad, suficiencia y calidad en la entrega y recolección del efectivo para el suministro a las oficinas y centros de pago y/o recaudo.</p> <p>Servicio Administración de Efectivo / Cajeros Automáticos Brindar medios diferentes a las oficinas para que nuestros clientes y/o usuarios puedan usar sus operaciones garantizando la oportunidad, suficiencia y calidad del dinero en el aprovisionamiento de efectivo de los cajeros automáticos.</p> <p>Servicio Administración de Efectivo / Cuadre Oficina Determinar que el saldo registrado en el sistema (aplicativo Canales) cuadre con el efectivo físico de la oficina, así como determinar la necesidad de éste que requiere la oficina para sus operaciones.</p>
	Informes	Dar cumplimiento oportuno a las normas establecidas por las entidades de control en cuanto a la generación y entrega de informes.

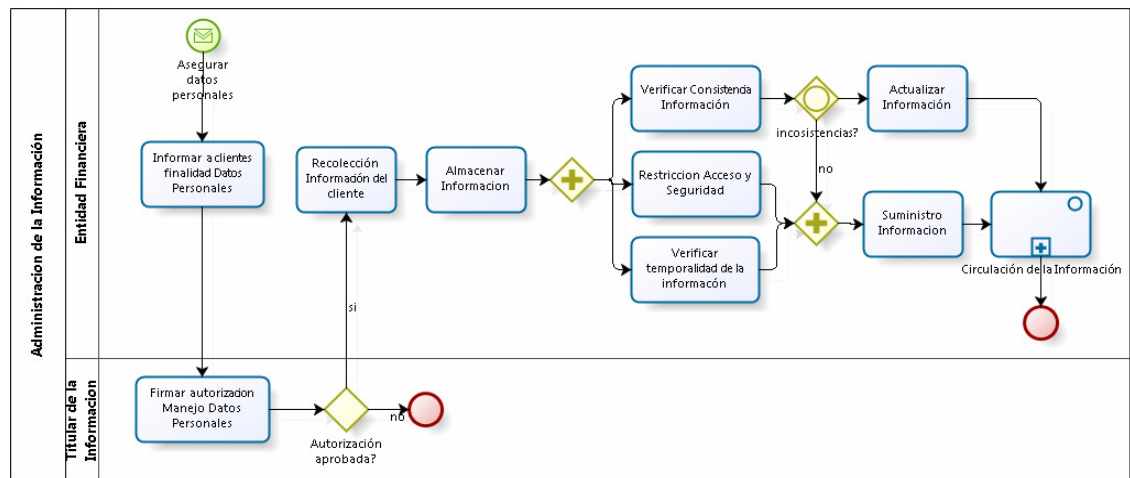
3.4.2 Macroproceso para la ejecución de la Ley Habeas Data. La ley estatutaria Habeas Data reglamenta los mecanismos para suministrar a los titulares de la información la posibilidad de reconocer y administrar la veracidad de los datos que a ellos se refieren. Para ello se definen los macroprocesos de Gestión de solicitudes de consultas y reclamaciones, Administración de la Información y Circulación de la información, los cuales se describen a continuación:

- **Macroproceso de Administración de la Información.** La gestión de datos personales debe obedecer a una finalidad específica, legitimizada por la constitución y las leyes. La finalidad de obtener datos personales y su posterior destinación debe darse a conocer claramente al titular de la información para que otorgue su autorización en dicho tratamiento.

La ley Habeas Data además de asegurar que los titulares autoricen la recolección de su información personal, restringe la circulación y acceso a la misma, disponiendo de mecanismos de control para validar que solo entidades permitidas conozcan esta información, y que a su vez estas cuenten con procesos internos que garanticen su protección. Las fuentes, operadores y usuarios de los registros personales deben proveer herramientas y procedimientos que den cuenta de la completa seguridad de la información

Una notación relevante esta en la prohibición de suministrar datos personales desactualizados que afecten así la finalidad y vulnerando derechos del titular. Así, con el objetivo de mantener la calidad de los registros o datos deben ejecutarse procesos para asegurar que la información contenida en los bancos de datos sea veraz, exacta y este actualizada.

El siguiente diagrama especifica los procesos encaminados a la administración de la información (finalidad, autorización, recolección, actualización, seguridad, confidencialidad y temporalidad de los datos personales) a la luz de la ley Habeas Data y su discernimiento a través del modelamiento de procesos empresariales:



[Fuente: Propia]

Ilustración 5: Diagrama de Administración de la Información

- **Macroproceso de Circulación de la Información**

¿Quiénes pueden disponer de los datos personales de los titulares almacenados en los bancos de datos de fuentes, operadores y usuarios?

La ley Habeas Data es clara en este sentido, y define que entidades y bajo que lineamientos pueden acceder a dicha información. La legitimidad en la finalidad de los accesos solicitados, que las entidades que acceden cuenten con autorización y mecanismos internos que extiendan el haber de la protección de los datos personales, y la relevancia en procesos judiciales o disciplinarios son algunas de las direcciones a evaluar para el tratamiento en el suministro de los datos.

Aquí, en este gráfico, se detallan los procesos generales que rigen el principio de circulación de la información:

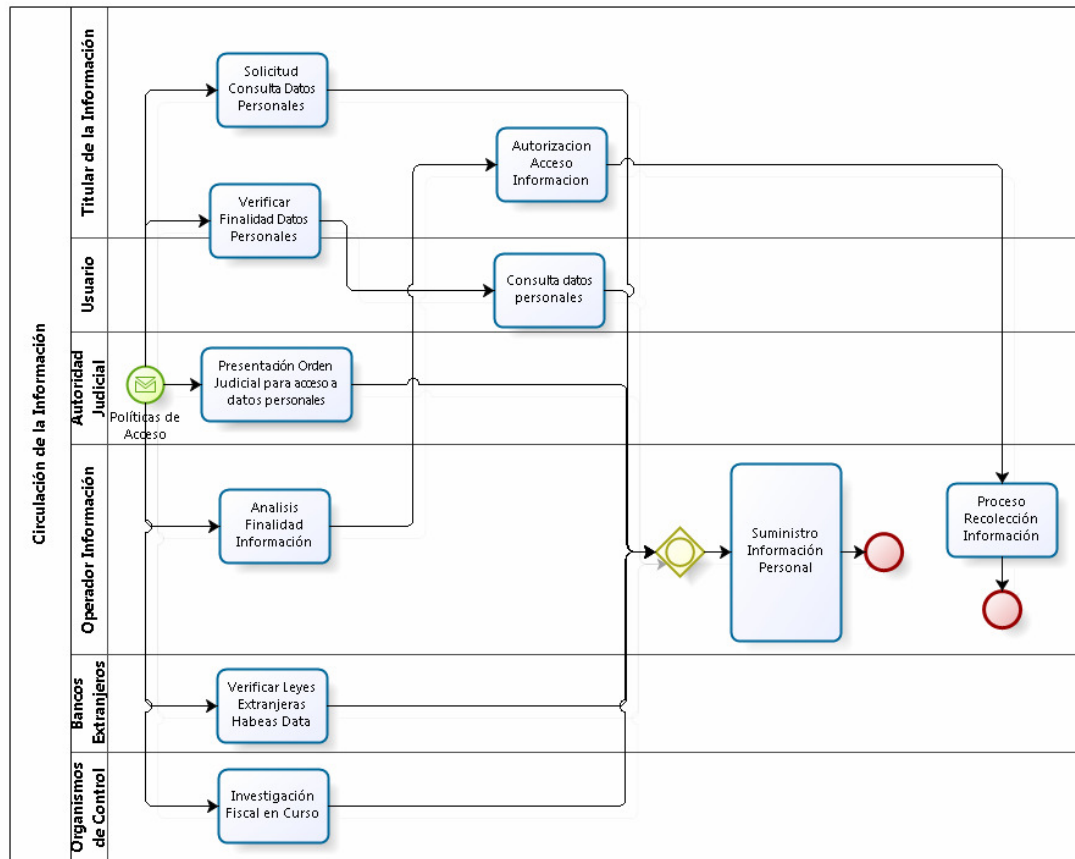


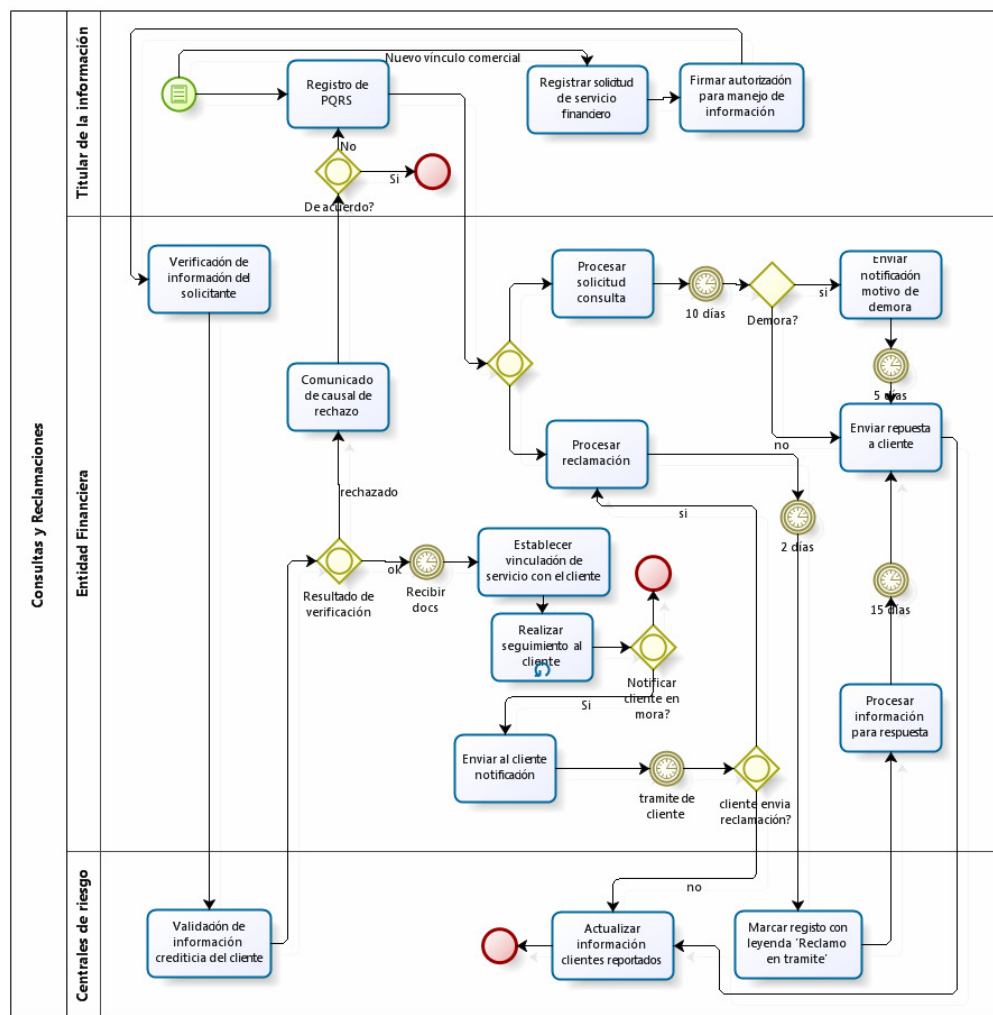
Ilustración 6: Proceso de Circulación de la Información.

3.4.2.1 Macroproceso de Gestión de Consultas y Reclamaciones

Para atender la vulnerabilidad de las personas ante entidades que no tenían procesos para proteger sus datos, actualizarlos, y evitar que la manipulación que éstas hacían de su información fuera en detrimento de sus derechos fundamentales, la ley habeas data regula el establecimiento de consultas, peticiones, reclamos, demandas por parte de los titulares de la información, imponiendo períodos y plazos fijos de respuesta.

Es relevante mencionar que una vez el titular inicia un proceso de reclamación, la marcación de su registro es informada a las diferentes fuentes de información y centrales de riesgo. Conformándose de esta forma una entidad única de información, en consonancia con la situación actual o en proceso de verificación.

En el siguiente diagrama se definen los actores y sus interacciones con los respectivos procesos PQRS, identificando el flujo de acción, la ejecución de las actividades y la notificación de cada resolución según la petición impuesta por el titular.



[Fuente: Propia]

Ilustración 7: Proceso de consultas y reclamaciones

3.4.3 Proceso: Comunicación a clientes morosos

Para cumplir con el estatuto, las entidades financieras deben enviar al domicilio de los clientes que presenten días de mora en sus obligaciones de tarjeta de crédito, créditos ML, créditos ME y/o sobregiros, un comunicado que informe el estado en que se encuentran sus obligaciones, antes de reportarlo como moroso a las centrales de riesgo, con el objetivo de cumplir lo establecido por el artículo 12 de la Ley Habeas Data sobre el reporte de información negativa referente al incumplimiento de obligaciones por parte de sus clientes.

- **Especificación general del proceso: Comunicación a clientes morosos**

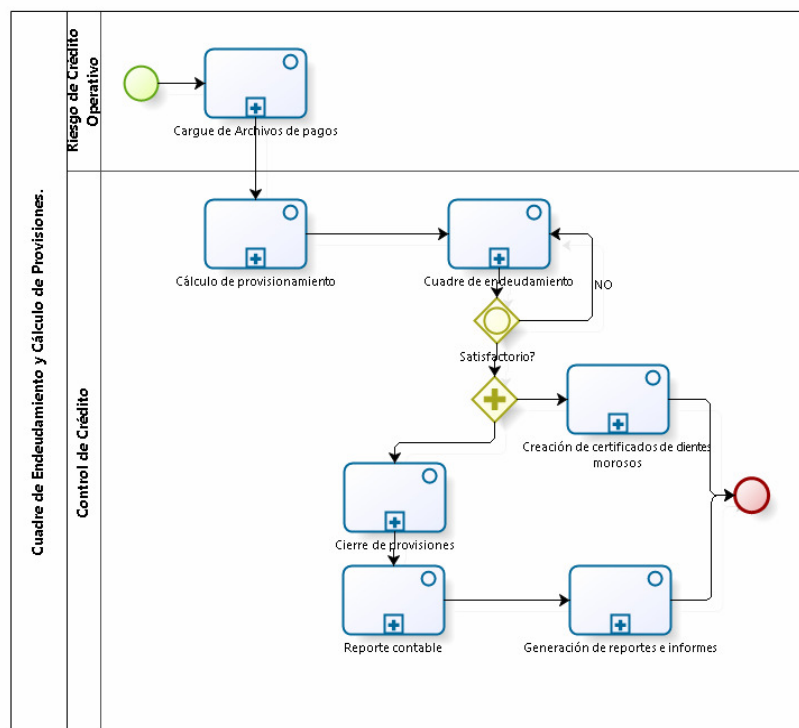


Ilustración 8: Proceso de comunicación a clientes morosos

3.4.3.1 Requerimientos del proceso

<p>Generar archivo de clientes con obligaciones en mora</p>	<p>SARC debe desarrollar una funcionalidad para generar un archivo que contenga el registro de los clientes que tienen obligaciones en mora.</p> <p>El archivo debe contener los siguientes datos:</p> <ul style="list-style-type: none"> • Número de Identificación del cliente • Tipo de identificación del cliente • Nombre del cliente • Dirección de correspondencia. • Código DANE de la dirección de correspondencia. • Mensaje (parametrizado). <p>El contenido del archivo, debe corresponder a:</p> <ul style="list-style-type: none"> • Obligaciones correspondientes al mes de la última generación del cuadro de endeudamiento. • Se debe tener un registro por cliente. Es decir, que si un cliente tiene cinco obligaciones en mora para ser reportadas a las centrales de riesgo, el archivo debe contener un solo registro del cliente. • El Core Bancario o la solución tecnológica que representa el corazón de los procesos de la entidad financiera, debe enviar al SARC el registro de las obligaciones vencidas por pago de cartera. • El sistema CRM de la entidad financiera debe reportar el domicilio actual del cliente al que se le deba enviar comunicación por mora.
<p>Parametrización</p>	<p>Se debe permitir al usuario parametrizar los siguientes datos:</p>

de datos	<ul style="list-style-type: none"> El límite de días en que una obligación o producto debe tener de mora para ser reportado a las centrales de riesgo. Mensaje del comunicado enviado al cliente moroso.
Administración de registros de clientes en mora	<p>Se requiere de un servicio en el cual el usuario pueda:</p> <ul style="list-style-type: none"> Adicionar y eliminar registros del archivo de clientes en mora. Consultar historial de comunicaciones enviadas a un cliente.

- Casos de uso arquitectónicamente significativos**

Caso de Uso	CU - Registrar Parámetros Comunicado Habeas Data en SARC
Descripción	El sistema deberá permitir al administrador de SARC, registrar los parámetros para el comunicado de Habeas Data.
Flujo Básico de Eventos	<ol style="list-style-type: none"> El administrador de la aplicación SARC debe ingresar a la opción de parametrización para informes Habeas Data. El sistema debe mostrar en modo consulta, los siguientes datos: <ul style="list-style-type: none"> Fecha inicial Código Producto Días mínimo mora Días máximo mora Días resta sobregiros

	<ul style="list-style-type: none"> ○ Mensaje comunicado ○ Mensaje Codeudores <p>3. Si ya tiene información los parámetros ó si es la primera vez que se va a ingresar, debe seleccionar el registro que se desee modificar, actualizar la información capturada en la base de datos y almacenar los cambios para que se refleje la modificación realizada sobre la grilla de parámetros actuales.</p>
Flujo Alternativo	<p>3.1 Eliminar registros de parametrización</p> <p>3.1.1 Para eliminar algún parámetro, se debe seleccionar el registro que se desea eliminar y pulsar la opción de borrado.</p> <p>3.1.2 El sistema debe solicitar confirmación para eliminar el registro.</p> <p>3.1.3 El administrador del sistema debe aceptar la confirmación para continuar con el proceso.</p> <p>3.1.4 El sistema debe informar las dependencias existentes sobre el registro.</p> <p>3.1.5 El administrador debe verificar las dependencias y aceptar la eliminación.</p> <p>3.1.6 El sistema elimina el registro y actualiza la grilla de parametrización.</p>
Frecuencia de ocurrencia	Según las necesidades de los procesos de negocio.
Requerimientos especiales	Generar rastros de auditoría al adicionar, eliminar o modificar un parámetro.

Caso de Uso	CU - Generar Población de Clientes y/o Codeudores Morosos
Descripción	El sistema deberá permitir al auxiliar de Control de Crédito, generar la población de los clientes y/o codeudores que tiene cartera morosa para enviar comunicado de posible reporte

	negativo en las centrales de riesgo.
<i>Precondiciones</i>	<ul style="list-style-type: none"> • El cuadre de endeudamiento debe haber sido generado satisfactoriamente. • Parametrización Habeas Data en el sistema SARC.
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1. El Auxiliar de Control y Crédito ingresa a la opción del SARC que permite la generación del archivo de clientes morosos e inicia el proceso. 2. El sistema SARC debe generar un archivo con la población de clientes que tengan obligaciones que son iguales o exceden el número de días de mora de capital definidas por la entidad y parametrizados en el SARC. Cuando la parametrización del producto lo defina, se debe asociar el codeudor del cliente a la población de registros. 3. Una vez se genera la población de clientes, el sistema debe enviar un correo electrónico al buzón del auxiliar de Control de Crédito, indicando los siguientes datos: <ul style="list-style-type: none"> ○ Estado del proceso ○ Mes de corte generado ○ Cantidad de clientes en le informe generado ○ Cantidad de codeudores en el informe generado
<i>Poscondiciones</i>	Generar archivo de clientes morosos.
<i>Frecuencia de ocurrencia</i>	Este caso de uso debe poderse ejecutar la veces que se quiera, teniendo en cuenta que no se deben perder las adiciones o eliminaciones realizadas por el usuario en el mismo mes de corte.
<i>Requerimientos especiales</i>	<ul style="list-style-type: none"> • Se deben generar rastros de auditoria de generación del evento. • El primer proceso de generación de la población, debe incluir las siguientes características: <ul style="list-style-type: none"> ○ Clientes con obligaciones castigadas con saldo pendiente por recuperar.

	<ul style="list-style-type: none"> ○ Clientes con obligaciones con días de mora mayores o iguales a 1. ○ Clientes sin obligaciones prescriptas.
--	---

Caso de Uso	CU - Generar Archivo de Clientes para SARC
<i>Descripción</i>	El sistema de gestión centralizada de clientes, deberá permitir al operador del centro de cómputo, generar un archivo con la información básica de los clientes.
<i>Precondiciones</i>	Se parte de la premisa de tener un sistema centralizado para la administración de la información del cliente como un CRM. En caso que la información del cliente se encuentre distribuida en varias aplicaciones, la entidad debe validar la manera de consolidar la información de los clientes para la fecha seleccionada en único archivo. El manejo de las integraciones requeridas para generar el consolidado, se encuentran por fuera del alcance del proyecto.
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1. El Operador del centro de cómputo de la entidad debe acceder al sistema CRM o la aplicación que administre la información de los clientes y ejecutar la generación del archivo de clientes para una fecha determinada. 2. El sistema debe generar un archivo con todos los clientes actuales en la base de datos hasta la fecha de corte ingresada por el usuario. La información mínima que debe contener el archivo es la siguiente: <ul style="list-style-type: none"> • Tipo de Registro: Indicador de registro de detalle • Tipo de Persona: Persona natural y jurídica • Segmento de Banca: Banca persona, empresarial u otras según definan • Cliente: Nombre de cliente

	<ul style="list-style-type: none"> • Código Industrial Internacional Uniforme (CIIU) [37]: Datos del CIIU correspondiente al cliente según la tabla del DANE. • Sexo: Masculino, femenino y empresa. • Fecha de nacimiento: Fecha de nacimiento del cliente • Dirección de correspondencia: La dirección de correspondencia más reciente del cliente. • Ciudad de correspondencia: Código DANE de la ciudad de correspondencia del cliente. • Código de departamento: Código DANE del departamento al que pertenece la ciudad. • Naturaleza de cliente: Se identifica si el cliente es personal o empresarial. En caso que el cliente sea empresarial, se identifica el código de naturaleza del cliente: consorcio, entidad pública, sin ánimo de lucro, anónima, entre otros. • Fecha de constitución: Solo aplica para los clientes empresariales. Se reporta la fecha de registro de la empresa en Cámara de Comercio. • fecha vinculación: Fecha de vinculación con el banco o entidad financiera del cliente persona natural o empresarial.
3.	El archivo debe ser enviado al Sistema de Administración de Riesgos Crediticios SARC, dejándolo en un repositorio designado para ello.
4.	El sistema de gestión de usuarios debe notificar al usuario

	el estado del proceso.
<i>Poscondiciones</i>	Cargar archivo de clientes en SARC
<i>Frecuencia de ocurrencia</i>	Definida por el proceso. Se estima mensual y se recomienda el día 20 de cada mes.
<i>Requerimientos especiales</i>	Rastros de auditoria cuando el usuario genere el archivo, de tal manera que se pueda identificar quién y cuándo se realizó el evento

Caso de Uso	CU - Cargar archivo de clientes en SARC
<i>Descripción</i>	El sistema deberá permitir al administrador del SARC, cargar el archivos de clientes.
<i>Precondiciones</i>	Desde el sistema de gestión de clientes se debió generar un archivo de datos básicos de clientes y enviarlo al repositorio de SARC.
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1 El Administrador del SARC debe ingresar por una opción del sistema que permita seleccionar el archivo de clientes a procesar. 2 El sistema debe procesar el archivo seleccionado. 3 Una vez el sistema termine el procesamiento de la información, debe mostrarle al usuario un log de los rechazos obtenidos del cargue. 4 El usuario debe tener la opción de almacenar u omitir el archivo de cargue del sistema. <p>•</p>
<i>Frecuencia de ocurrencia</i>	Definida por el proceso. Se estima mensuale y se recomienda el día 20 de cada mes.

Caso de Uso	CU - Generar Población de Clientes y/o Codeudores Morosos	
<i>Descripción</i>	El sistema deberá permitir al auxiliar de Control de Crédito, generar la lista de los elementos de la población de los clientes y/o codeudores que tiene cartera morosa para enviar comunicado de posible reporte negativo en las centrales de riesgos.	
<i>Precondiciones</i>	Cuadre del endeudamiento realizado satisfactoriamente. Parámetros capturados en el sistema SARC.	
<i>Flujo Básico de Eventos</i>	1	El auxiliar de Control y Crédito debe acceder a la aplicación SARC y estando en el menú principal ingresar a la opción o ruta que permite generar la población de clientes morosos.
	2	Una vez el sistema SARC despliega la pantalla para iniciar el proceso de generación de los clientes morosos, se debe comenzar el procesamiento.
	3	Una vez ejecutado el paso anterior, genere la lista de los clientes que cumplen con alguna de las siguientes condiciones: <ul style="list-style-type: none"> • Clientes con obligaciones con días de mora capital dentro del rango de días definidos por el parámetro. • Clientes con obligaciones que sorpresivamente aparecen con días de mora capital menor al parámetro definido para este fin y que en el mes anterior no tenía días de mora. • Codeudores que estén asociados a la obligación del deudor o cliente, siempre y cuando el parámetro del producto lo defina. • En el caso de los sobregiros se deberán restar a los días de mora los días definidos según la parametrización, para identificar realmente los días de mora.
	4	Una vez terminado el procesamiento, se debe enviar un correo electrónico al buzón del auxiliar de Control de Crédito, indicando los siguientes datos:

	<ul style="list-style-type: none"> • Estado del proceso • Mes de corte generado • Cantidad de clientes incluidos en el informe • Cantidad de codeudores incluidos en el informe
<i>Poscondiciones</i>	Listado de clientes detectados como morosos.
<i>Frecuencia de ocurrencia</i>	Este caso de uso debe poderse ejecutar la veces que se quiera, teniendo en cuenta que no se deben perder las adiciones o eliminaciones realizadas por el usuario en el mismo mes de corte.
<i>Requerimientos especiales</i>	<p>Generar rastros de auditoria cuando el usuario genere el archivo, de tal manera que se pueda identificar quién y cuándo realizó el evento.</p> <p>Se requiere que el primer proceso de generación de la población, incluya los clientes con las siguientes características:</p> <p>Clientes con obligaciones castigadas con saldo pendiente por recuperar.</p> <ul style="list-style-type: none"> • Clientes con obligaciones con días de mora mayores o iguales a 1 • Clientes sin obligaciones prescriptas.

<i>Caso de Uso</i>	CU - Modificar registros al archivo de clientes y/o codeudores Morosos
<i>Descripción</i>	El sistema deberá permitir al auxiliar de Control de Crédito, adicionar y/o eliminar registros al archivo de clientes y/o codeudores morosos para enviar comunicado de posible reporte en las centrales de riesgo.
<i>Flujo Básico de Eventos</i>	<p>1 El auxiliar de control y crédito debe preparar un archivo, con los siguientes datos:</p> <ul style="list-style-type: none"> • Identificación del cliente • Tipo de identificación del cliente • Tipo Novedad • Observación (justificación de la adición o eliminación) • Tipo Cliente

	<p>2 El analista debe ingresar a la opción del SARC para modificar un registro del archivo de clientes y/o codeudores morosos. Desde esta opción se debe seleccionar el mes de corte a modificar y seleccionar la ruta del archivo generado con antelación.</p> <p>3 Una vez capturados los datos descritos en el paso anterior, oprima el botón IMPORTAR ARCHIVO para que el sistema SARC realice los siguientes pasos:</p> <ul style="list-style-type: none"> • Los registros deben corresponder a la estructura definida para el archivo definido en el primer paso. • Para adicionar un registro se debe validar que el cliente o codeudor no exista en la población previamente identificada para enviar comunicación. • Para eliminar un registro se debe validar que el cliente o codeudor realmente exista en la población previamente identificada para enviar comunicación del mes correspondiente. <p>4 Si el archivo no presenta inconsistencias, debe generar un tipo de novedad acorde con la operación realizada.</p> <p>5 Además debe quedar rastro de quién modificó el registro.</p> <p>6 Si la modificación fue una adición, se debe adicionar el registro a la población correspondiente al mes de corte del endeudamiento. En caso que la modificación sea un borrado, se elimina el registro del mes seleccionado siempre y cuando pertenezca al mes de corte del endeudamiento. Por ejemplo si el mes de corte es Febrero/09 y el usuario seleccionó Enero/09, no se puede borrar porque el mes seleccionado no corresponde al mes de corte.</p> <p>7 Una vez terminado el paso anterior, envíe un correo electrónico al buzón del auxiliar de Control de Crédito, indicando los siguientes datos:</p> <ul style="list-style-type: none"> • Estado del proceso • Mes de corte procesado • Cantidad de clientes adicionados • Cantidad de clientes borrados • Cantidad de clientes rechazados
--	---

	<ul style="list-style-type: none"> • Cantidad de codeudores adicionados • Cantidad de codeudores borrados • Cantidad de codeudores rechazados • Link de acceso al archivo de clientes y/o codeudores rechazados
<i>Flujo Alterno</i>	<p>3.2 Si en el paso anterior se detectan registros inconsistentes, notifique al usuario los registros que están inconsistentes e informe que el archivo no puede ser cargado y debe ser corregido.</p> <p>3.3 Si el archivo presenta inconsistencias, no debe cargar ningún registro.</p>
<i>Poscondiciones</i>	Generación de archivo de clientes morosos en el SARC.
<i>Frecuencia de ocurrencia</i>	Definido por la necesidad del proceso.
<i>Requerimientos especiales</i>	Dejar rastros de auditoria cuando el usuario adicione o elimine un registro del archivo, de tal manera que se pueda identificar quién y cuándo realizó el evento.

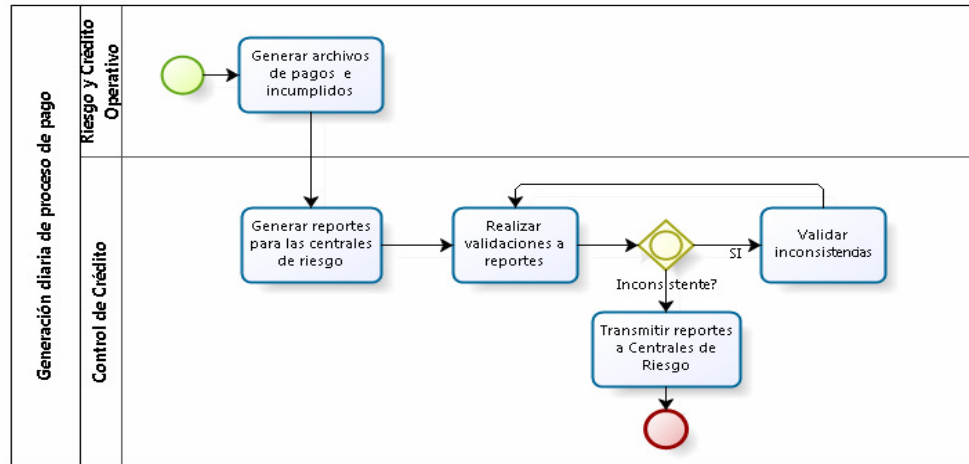
Caso de Uso	CU - Consultar historia de envío de comunicaciones
<i>Descripción</i>	Técnico - Procesos
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1. El auxiliar de control y crédito, debe acceder a la opción de SARC que permite consultar la historia de envío de comunicaciones a un cliente. 2. Se debe seleccionar los parámetros por los cuales se desea realizar la consulta. 3. El sistema debe generar la consulta según los parámetros ingresados por el usuario. 4. El sistema procesa la consulta y debe mostrar en pantalla la lista de los meses (día - mes - año) en la cual se han enviado comunicaciones al cliente ingresado por el auxiliar de control de crédito.

<i>Flujo Alterno</i>	<p>2.1 Si desea consultar por identificación se debe mostrar un sistema que filtre la consulta por los siguientes campos: Identificación y tipo de identificación</p> <p>2.2 Si desea consultar por nombre, el sistema debe mostrar una pantalla en la cual el auxiliar pueda filtrar la consulta por el campo Nombre.</p>
<i>Frecuencia de ocurrencia</i>	Cada vez que se ejecute el proceso.

3.4.4 Proceso: Generación diaria de archivos de pagos

Actualmente el sistema SARC de la entidad financiera debe generar el reporte diario de pagos a las centrales de riesgo, pero no se emite diariamente, sino de manera quincenal. Por tal motivo, para cumplir con el numeral 1 del artículo 8 de la ley Habeas Data en dónde se establece que “las fuentes de la información deben garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada, y comprobable” [7], se debe modificar la funcionalidad que actualmente provee el SARC para generar con mayor frecuencia el reporte de pagos de Cartera Total que se envía a las centrales de riesgo, con la nueva estructura del archivo definida por la CIFIN.

3.4.4.1 Especificación general del proceso: Generación diaria de archivos



powered by
 Bizagi
 Process Modeler

[Fuente: Propia]

Ilustración 9: Proceso de generación diaria de proceso de pago

- **Casos de uso arquitectónicamente significativos**

Caso de Uso	CU - Generar archivos de pagos e incumplidos
<i>Descripción</i>	El sistema core bancario de la entidad financiera deberá generar archivos diarios en dónde se reporte los pagos realizados en un período de tiempo y las obligaciones incumplidas.
<i>Precondiciones</i>	<p>La entidad financiera debe contar con un sistema para la gestión de la cartera, desde el cual se debe generar un archivo diario que contiene los pagos realizados y las obligaciones incumplidas.</p> <p>Generación de los procesos de aplicación de pagos acostumbrados y cierre diario.</p>

<i>Flujo Básico de Eventos</i>	<p>1 El sistema de cartera debe generar de manera automática dos archivos: uno para los pagos generados al día y otro para las obligaciones incumplidas. Se debe considerar que el periodo de generación debe ser desde el primer día calendario del mes, hasta el día anterior a la generación. Es decir, si el proceso se ejecuta el día 9 de abril, el rango de fechas debe ser: Fecha inicial: 01/04/2009, fecha final: 08/04/2009.</p> <p>2 El sistema debe procesar la información y generar los archivos de pagos recibidos y obligaciones incumplidas en el rango de fecha ingresado por el usuario. Los campos se describen:</p> <ul style="list-style-type: none"> • Nombre del cliente • Nit del cliente • Obligación incumplida (producto) • Días de mora <p>3 Una vez ejecutado el proceso, se debe generar una bitácora (log) que describe el resultado del proceso.</p> <p>4 El sistema debe enviar los archivos generados al sistema SARC de la entidad.</p> <p>5 El sistema SARC debe procesar la información de los archivos de pagos y obligaciones incumplidas recibidas, cargándola en su sistema.</p> <p>6 El sistema SARC debe generar una bitácora (log) que registre las inconsistencias encontradas.</p>
<i>Flujo Alterno</i>	<p>3.1. Si el resultado del proceso es no exitoso, se debe enviar una notificación al analista de cartera para que genere el archivo de manera manual, ingresando a la opción Generación de Archivo de Pagos, especificando el rango de fechas para la generación del archivo.</p> <p>5.1 Cuando el procesamiento de los archivos detecta inconsistencias, se debe enviar una notificación al analista de cartera para que cargue los archivos de manera manual, ingresando a la opción que SARC disponga para ello.</p>
<i>Frecuencia de ocurrencia</i>	Diaria.

<i>Requerimientos especiales</i>	<ul style="list-style-type: none"> Se deben incluir los pagos y las reversiones del mes. Las reversiones se pueden originar por devoluciones, o pagos mal aplicados.
----------------------------------	---

Caso de Uso	CU - Parametrizar información para el cifrado de archivos en SARC	
<i>Descripción</i>	El administrador de SARC debe registrar los parámetros para encriptar archivos de las centrales de riesgo.	
<i>Flujo Básico de Eventos</i>	1	El administrador SARC, accede a la opción del Sistema de Administración de Riesgo Crediticio – SARC que permite administrar las claves necesarias para enviar reportes encriptados a las centrales de riesgo.
	2	El sistema debe desplegar en modo consulta la siguiente información: Código proceso, nombre del archivo, proveedor o tercero y aplicación para encriptar. a. NOTA: La Circular Externa 052 del 2007 emitida por la Superintendencia Financiera [38] exige a las entidades financieras disponer de herramientas de Certificación de Seguridad de alto nivel, por lo cual las claves deben ser encriptadas con llaves publicas y privadas a través de dichas herramientas.
	3	El administrador del sistema selecciona la opción de actualizar, adicionar o eliminar los campos de parametrización.
	4	El sistema actualiza la información de los parámetros modificados.
<i>Flujo Alternativo</i>	3.1 El usuario adiciona nuevos parámetros. 3.1.1 El usuario selecciona la opción de adicionar para habilitar los campos: Código proceso, nombre del archivo, proveedor o tercero y aplicación para encriptar. 3.1.2 El usuario registra la nueva información a los campos.	

	<p>3.1.3 El usuario confirma almacenar la parametrización.</p> <p>3.1.4 El sistema almacena la información capturada en la base de datos.</p> <p>3.2 EL administrador del SARC selecciona la opción de modificar parámetros, siguiendo los siguientes pasos:</p> <p>3.2.1 Selecciona en la grilla de datos de los Parámetros Actuales, el registro que desea.</p> <p>3.2.2 Modifica cualquiera de los campos desplegados por el sistema (Código del proceso, nombre del archivo, proveedor o tercero y aplicación para encriptar).</p> <p>3.2.3 Confirma la solicitud de almacenar los cambios generados.</p> <p>3.2.4 El sistema actualiza la información capturada en la base de datos.</p> <p>3.2.5 Se actualiza la información de los datos de la grilla de Parámetros Actuales capturados en la pantalla.</p> <p>3.3 El administrador SARC selecciona la opción de eliminar parámetros, siguiendo los siguientes pasos:</p> <p>3.3.1 Seleccionar en la grilla de datos de los Parámetros Actuales, el registro que se desea eliminar.</p> <p>3.3.2 El sistema muestre un mensaje de solicitud de confirmación al usuario si realmente desea eliminar el registro.</p> <p>3.3.3 El usuario confirma la acción de eliminación para el registro seleccionado.</p> <p>3.3.4 El sistema elimina de la base de datos el registro seleccionado por el usuario.</p> <p>3.3.5 El sistema actualiza la grilla de Parámetros Actuales desplegada en el sistema.</p>
<i>Requerimientos especiales</i>	Generar rastros de auditoria cuando el administrador del SARC adicione, elimine o modifique algún parámetro, de tal manera que se pueda identificar quién y cuándo realizó el evento

Caso de Uso	CU - Encriptar archivos para su envío de centrales de riesgo
Descripción	<p>El sistema debe encriptar un archivo antes de enviarlo a las centrales de riesgo.</p> <p>Cabe aclarar que para dar cumplimiento a la Circular Externa 052 del 2007 emitida por la Superintendencia Financiera, se debe generar un cifrado fuerte basado en “técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES” [38].</p>
Precondiciones	Generar reporte de pagos para las centrales de riesgo.
Flujo Básico de Eventos	<ol style="list-style-type: none"> 1 Cada archivo que deba ser reportado a las centrales de riesgo deben tener un código de proceso asociado y establecido en los parámetros de encriptación del sistema. 2 El sistema debe identificar el código del proceso y relacionar la llave o clave correspondiente al parámetro asignado. 3 El sistema debe encriptar el archivo según la llave o clave relacionada, utilizando el programa de encriptación parametrizado sobre el archivo correspondiente.
Poscondiciones	<p>Enviar archivo encriptado a centrales de riesgo.</p> <p>El archivo encriptado debe viajar a través de canales seguros y no debe tener ningún tipo de almacenamiento.</p> <p>La información desde la cual se genera el archivo, debe residir en la base de datos, asegurándose que la información confidencial se encuentra cifrada a través del mecanismo que considere la entidad financiera para tal fin.</p> <p>Los registros reportados deben ser identificables a través de la información contenida en la base de datos.</p> <p>Se debe generar registros de auditoría de los archivos enviados y la confirmación del acuse de recibo de la central de riesgo a la</p>

		que se reporta.
Frecuencia de ocurrencia		Diaria.

3.4.5 Proceso: Novedades de los reportes a las centrales de riesgo

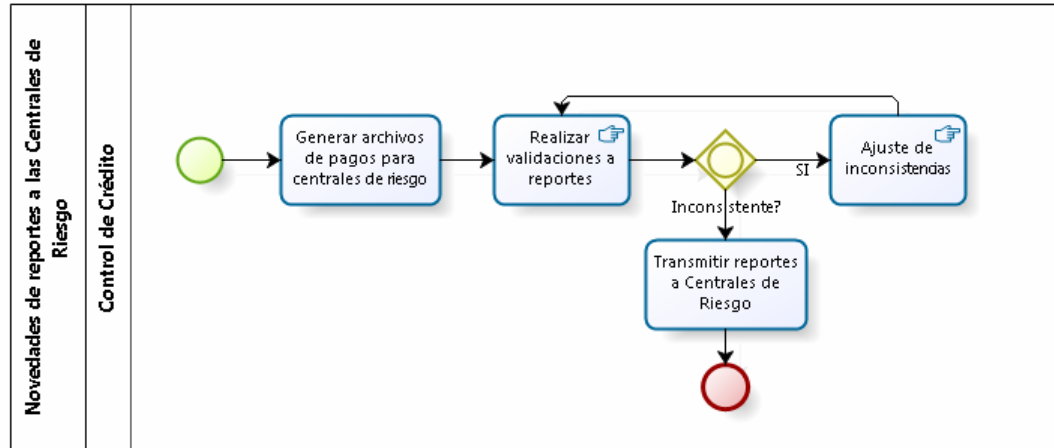
Crear una funcionalidad en SARC que permita modificar el universo de obligaciones que se envían en reporte mensual y de pagos de Cartera Total, Tarjeta de Crédito Visa y Master Card, con el fin de corregir las inconsistencias o rechazos reportados por las centrales de riesgo. La nueva funcionalidad debe poderse ejecutar en cualquier momento, es decir, antes y/o después de ser enviados los reportes a las centrales de riesgo correspondientes.

Según lo establecido en el numeral 3 del artículo 8 de la ley estatutaria 1266, Habeas Data, se reglamenta que: “Las fuentes de la información deben rectificar la información cuando sea correcta e informar lo pertinente a los operadores”.

Se entiende como Fuente de Información la entidad que recibe o conoce datos personales de los titulares de la información (Clientes), en virtud de una relación comercial o de servicio o de cualquier índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.

Se denomina Operador de Información a la entidad (Cifin y Data Crédito) que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley.

3.4.5.1 Especificación general del proceso: Novedades de los reportes a las centrales de riesgo



[Fuente: Propia]

Ilustración 10: Proceso de reporte de novedades a centrales de riesgo

- Casos de uso arquitectónicamente significativos**

<i>Caso de Uso</i>	CU – Parametrizar Plantilla para las Novedades de los Reportes de las Centrales de Riesgo
<i>Descripción</i>	El sistema deberá permitir al Oficial de Control de Crédito, crea, modificar o eliminar plantillas para las novedades de los reportes de las centrales de riesgo.
<i>Flujo Básico de Eventos</i>	1. El oficial de control de crédito debe ingresar a la opción del SARC que permite parametrizar la plantilla de novedades para los reportes de las centrales de riesgo.

	<p>2. El sistema deberá permitir al Oficial de Control de Crédito, crear, modificar o eliminar plantillas para las novedades de los reportes de las centrales de riesgo</p> <p>3. El Oficial de Control y Crédito debe seleccionar la opción requerida, generar la parametrización y almacenar los cambios.</p>
<i>Flujo Alterno</i>	<p>3.1 El Oficial de Control y Crédito selecciona la opción de crear una nueva plantilla.</p> <p>3.1.1 Una vez el sistema muestre la pantalla, ingrese en el campo Plantilla, el nombre de la plantilla que desea crear.</p> <p>3.1.2 El sistema debe mostrar en pantalla la lista de campos que se envían en los siguientes reportes: Reporte Mensual Cartera Total, Reporte Pagos Cartera Total, Reporte Mensual Tarjeta de Crédito y Reporte Pagos Tarjeta de Crédito.</p> <p>3.1.3 Se seleccionan los campos que contendrá la nueva plantilla.</p> <p>3.1.4 Se debe almacenar los cambios para que los campos seleccionados queden asociados a la nueva plantilla.</p> <p>3.2 El Oficial de Control y Crédito selecciona la opción de modificación a plantilla existente.</p> <p>3.2.1 Se selecciona la plantilla que se desea modificar.</p> <p>3.2.2 El sistema muestra los datos asociados a la plantilla seleccionada por el usuario en modo consulta. De igual manera muestre en pantalla la lista de campos que se envían en los siguientes reportes: Reporte Mensual Cartera Total, Reporte Pagos Cartera Total, Reporte Mensual Tarjeta de Crédito y Reporte Pagos Tarjeta de Crédito.</p> <p>3.2.3 El usuario debe seleccionar la opción modificar para que el sistema habilite los campos que tenga actualmente la plantilla seleccionada.</p> <p>3.2.4 Una vez ejecutado el paso anterior, se deben realizar las</p>

	<p>modificaciones necesarias (eliminar, adicionar) los campos que tiene actualmente la plantilla.</p> <p>3.2.5 Una vez ejecutado el paso anterior, oprima el botón GUARDAR, para que los campos seleccionados queden asociados a la nueva plantilla.</p> <p>3.3 El Oficial de Control y Crédito selecciona la opción de eliminar una plantilla existente.</p> <p>3.3.1 Se selecciona la plantilla que desea eliminar.</p> <p>3.3.2 El sistema despliega los campos correspondientes a la plantilla asociada para los reportes: Reporte Mensual Cartera Total, Reporte Pagos Cartera Total, Reporte Mensual Tarjeta de Crédito y Reporte Pagos Tarjeta de Crédito.</p> <p>3.3.3 El sistema muestra un mensaje confirmando al usuario si realmente desea eliminar la plantilla seleccionada.</p> <p>3.3.4 El usuario confirma la opción de eliminar la plantilla que seleccionó.</p> <p>3.3.5 El SARC elimina la plantilla de la base de datos.</p>
<i>Poscondiciones</i>	Generar rastros de auditoría cuando el usuario ejecute este caso de uso, de tal manera que se pueda identificar quién y cuándo realizó el evento.
<i>Frecuencia de ocurrencia</i>	Según la necesidad del negocio.
<i>Requerimientos especiales</i>	<ul style="list-style-type: none"> • Todas las plantillas nuevas deben tener obligatoriamente los siguiente campos: <ul style="list-style-type: none"> ○ Número de identificación ○ Número de obligación ○ Código de sucursal ○ Línea de Crédito

Caso de Uso	CU – Actualizar Obligaciones de los Reportes generados a las Centrales de Riesgo
<i>Descripción</i>	El sistema deberá permitir al Oficial de Control de Crédito, realizar modificaciones y eliminaciones masivas de los reportes de las centrales de riesgo.
<i>Precondiciones</i>	<p>Archivo de población de obligaciones para el reporte mensual y de pagos con los campos requeridos para la plantilla seleccionada.</p> <p>Parametrización de la plantilla correspondiente.</p>
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1. Oficial de Control y Crédito, desde la aplicación SARC acceda a la opción de actualización de reportes generados a las Centrales de Riesgo. 2. El sistema debe desplegar la siguiente información: <p>Tipo Reporte: Lista con los reportes disponibles. El usuario debe seleccionar el reporte sobre el cual desea realizar la novedad. Los reportes disponibles son: Reporte Mensual Cartera Total, Reporte Pagos Cartera Total, Reporte Mensual Tarjeta de Crédito Visa, Reporte Pagos Tarjeta de Crédito Visa, Reporte Mensual Tarjeta de Crédito MasterCard y Reporte Pagos Tarjeta de Crédito MasterCard.</p> <p>Plantilla: Lista con las plantillas asociadas al reporte seleccionado. El usuario debe seleccionar la plantilla a la que desea cargar información.</p> <p>Ubicación Archivo: Permite ingresar la ruta de ubicación física del archivo que contiene la información del reporte sobre el cual se quiere generar novedades.</p> 3. El usuario carga el archivo al sistema SARC. 4. El sistema procesa la información y realiza un cargue temporalmente del archivo según la plantilla seleccionada por el usuario. 5. El sistema despliega en pantalla los datos del archivo en

	<p>forma de grilla.</p> <p>6. Se valida el archivo cargado para que no tenga inconsistencias.</p> <p>7. Si el archivo no presenta registros con inconsistencias, el sistema carga el archivo en su base de datos.</p> <p>8. El usuario realiza las modificaciones correspondientes en el universo de obligaciones del reporte seleccionado por el usuario. La eliminación de los registros seleccionados por el usuario debe realizarse sólo de manera lógica.</p> <p>9. El usuario almacena los cambios.</p> <p>10. El sistema notifica al usuario la cantidad de registros procesados.</p>
<i>Flujo Alterno</i>	<p>6.1 Si el archivo presenta algún registro con inconsistencias, el sistema no realiza carga del archivo y genera un log de los registros con inconsistencia.</p> <p>8.1 Cuando se modifican los campos: Clasificación, fecha de pago, estado, cuotas en mora, años en mora, saldo, fecha de corte, estado de contrato, modo extinción y/o tipo de pago, el usuario debe indicar si la actualización aplica al reporte mensual o el de pagos.</p>
<i>Frecuencia de ocurrencia</i>	Según la necesidad del negocio.
<i>Requerimientos especiales</i>	<p>El archivo que se carga en el sistema puede contener uno o varios registros para ser modificados o eliminados.</p> <p>Existen campos de los reportes que requieren ser convertidos (recodificados), para ser enviados a las Centrales de Riesgo, el archivo tendrá los datos de aquellos campos, tal como se encuentran en la base de datos del SARC.</p> <p>Las modificaciones o eliminaciones deben realizarse sobre los universos o poblaciones de obligaciones correspondientes al último mes de corte sin importar si éste se encuentra cerrado o no.</p> <p>No se debe almacenar el registro histórico de las actualizaciones generadas. Se almacena únicamente el último</p>

	<p>evento ejecutado por el usuario.</p> <p>Debe quedar rastros de auditoría cuando el usuario modifique algún registro, de tal manera que se pueda identificar quién y cuándo realizó el evento.</p>
--	--

Caso de Uso	CU - Consultar reportes de la centrales de riesgo en SARC
<i>Descripción</i>	El Oficial de Control de Crédito, podrá consultar obligaciones registradas en los reportes de las centrales de riesgo.
<i>Precondiciones</i>	Generación del universo de obligaciones para el reporte mensual y de pagos.
<i>Flujo Básico de Eventos</i>	<ol style="list-style-type: none"> 1. El Oficial de Control y Crédito, accede a la opción del SARC que permite realizar consulta de reportes a las centrales de riesgo. 2. El usuario debe seleccionar los siguientes criterios de búsqueda: Tipo de Reporte (Reporte Mensual Cartera Total, Reporte Pagos Cartera Total, Reporte Mensual Tarjeta de Crédito, Reporte Pagos Tarjeta de Crédito), identificación o nombre. 3. El usuario indica al sistema que desea realizar la consulta. 4. El sistema procesa la información y despliega un listado de registros de clientes que coinciden con los parámetros de búsqueda ingresados por el usuario en el campo identificación o nombre. 5. El usuario selecciona uno de los clientes del listado de registros desplegados por el sistema para detallar sus obligaciones. 6. El sistema muestra en pantalla la lista de obligaciones correspondientes al cliente seleccionado, mostrando los siguientes campos:

Tipo de identificación	Valor de la garantía
Número de identificación	Obligación reestructurada
Nombre tercero	Naturaleza de la reestructuración
Reservado	Número de reestructuraciones
Número de la obligación	Clase de tarjeta (Débito, Crédito Visa, Crédito Mastercard)
Código sucursal	Número de cheques devueltos
Calidad	Categoría de los servicios
Calificación	Plazo
Situación o estado del titular	Días de cartera
Estado	Tipo de cuenta
Edad de mora o manejo	Cupo sobregiro
Años en mora	Días autorizados
Fecha de corte	Dirección residencia del tercero
Fecha inicial o expedición	Teléfono residencia del tercero
Fecha terminación	Código ciudad de residencia
Fecha de exigibilidad	Nombre ciudad de residencia del tercero
Fecha de prescripción	Código departamento de residencia
Fecha de pago	Departamento residencia del tercero
Modo extinción	Nombre empresa

	Tipo de pago	Dirección de la empresa
	Periodicidad de pago	Teléfono de la empresa
	Probabilidad de no pago	Código ciudad empresa
	Número de cuotas pagadas	Ciudad empresa del tercero
	Número de cuotas pactadas	Código departamento empresa
	Cuotas en mora	Departamento empresa del tercero
	Valor o cupo	Fecha inicio excensión Gravamen de Movimiento Financiero (GMF)
	Valor de mora	Fecha terminación extensión Gravamen de Movimiento Financiero (GMF)
	Valor del saldo	Numero de renovación CDT.
	Valor de la cuota	Cuenta de ahorro exenta Gravamen de Movimiento Financiero (GMF).
	Valor de cargo fijo	Tipo de identificación originaria
	Línea de crédito	Número de identificación originaria
	Cláusula de permanencia	Tipo de entidad originaria
	Tipo de contrato	Código de entidad originaria
	Estado de contrato	Tipo de fideicomiso
	Termino o vigencia del contrato	Número del fideicomiso
	Numero de meses del contrato	Nombre fideicomiso
	Naturaleza jurídica	Tipo de deuda cartera
	Modalidad de crédito	Tipo de póliza

	Tipo de moneda	Código de ramo
	Tipo de garantía	Fecha última modificación
		Tipo novedad

3.4.6 Proceso: Marcación de reclamos en las centrales de riesgo

De acuerdo a la ley 1266 de Habeas Data del 31 de diciembre de 2008 se establece en el Título V, Artículo 16 Peticiones, Consultas y Reclamos, las reglas para el trámite y atención de los reclamos que presenten los clientes ante el operador o las fuentes cuando consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización.

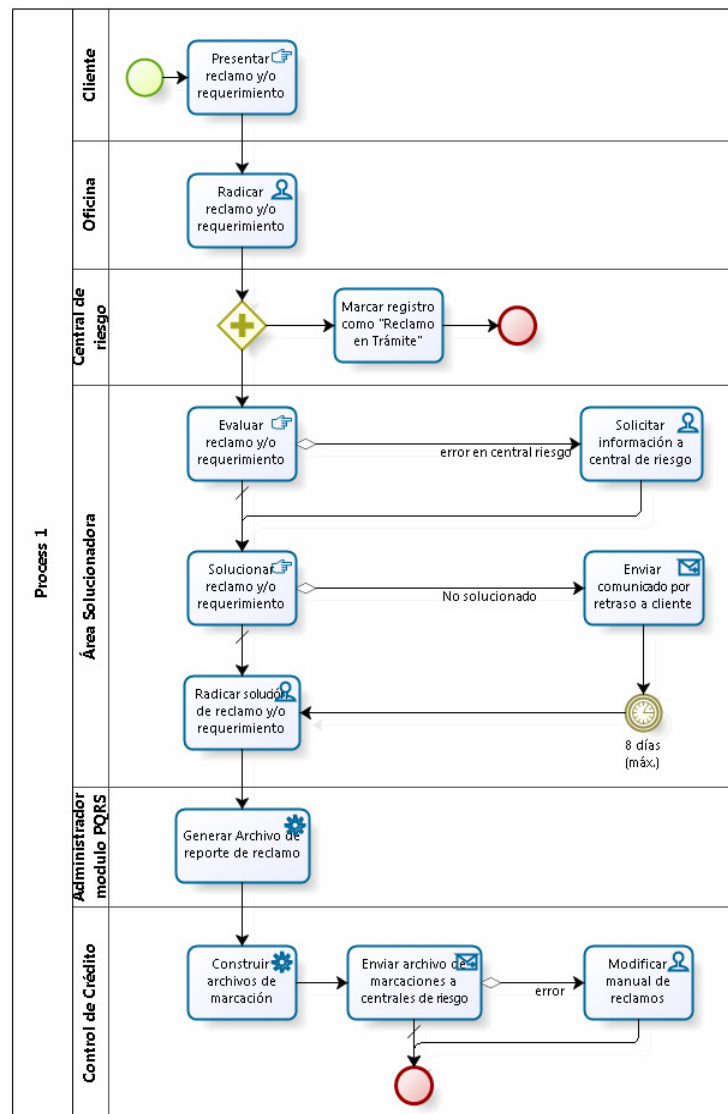
Cuando una persona encuentra un error en su registro individual, debe acercarse a la entidad financiera y radicar un reclamo que describa el inconveniente presentado. El reclamo presentado deberá ser informado en las centrales de riesgo (CIFIN y Datacrédito) para que, en un plazo máximo de 2 (dos) días, marquen el registro individual con la leyenda “reclamo en trámite” hasta que se resuelva la reclamación.

Toda reclamación debe ser resuelta en máximo 15 (quince) días hábiles. En caso de no poderse cumplir dicho plazo, la entidad financiera debe informar al afectado la razón de la demora y se permitirán ocho días hábiles más.

Actualmente, los reportes a Centrales de Riesgo (CIFIN y Datacrédito), que envía el Banco desde SARC, no tiene en cuenta los reclamos presentados por los clientes en oficina. Bajo la ley de Habeas Data, es necesario que el módulo de PQRS de la entidad financiera se integre con el SARC para que

los reclamos que se presenten a diario se puedan enviar a las centrales y se realice el marque y desmarque de acuerdo a lo estipulado en la ley.

- **Definición del general del proceso: Marcación de reclamos en las centrales de riesgo.**



[Fuente: Propia]

Ilustración 11: Proceso de marcación de reclamos a centrales de riesgo

- **Casos de uso arquitectónicamente significativos**

Caso de Uso	CU - Generar Archivo consolidado de reclamos
<i>Descripción</i>	El sistema debe generar y enviar al SARC de forma automática, el reporte de los reclamos que exigen el marque y desmarque en centrales de riesgo y que fueron presentados en el día por los clientes por medio del sistema de manejo de reclamaciones que disponga la entidad financiera.
<i>Precondiciones</i>	<p>El sistema de administración de reclamos de la entidad financiera debe tener parametrizado los siguientes criterios:</p> <p>Número de obligación 'Crédito no suministrado' o la etiqueta que la entidad considere para hacer la correspondiente referencia.</p> <p>Asociar los productos que ofrecen la entidad financiera y que pueden ser objetos de reclamaciones de acuerdo con la ley de Habeas Data.</p> <p>Agregar atribuciones especiales (subtipo de respuesta - subtipo de expediente) para aquellos reclamos que exigen marcación en centrales de riesgo con las opciones: Actualización, corrección, eliminación, ratificación y prórroga.</p> <p>Para tipos de reclamo de Actualización y Corrección, se debe asociar la siguiente parametrización de Subtipo de reclamo:</p> <p>Obligación al día</p> <p>Obligación a paz y salvo</p> <p>Desembargo de cuenta</p> <p>Prescripción SU 082 (derecho a la información y buen nombre)</p> <p>Prescripción T 284 (Hábeas Data, caducidad del dato referido a obligaciones impagas)</p> <p>Permanencia de la información</p>

	<p>GMF (Gravamen de Movimiento financiero) marcación y desmarcación</p> <p>Calificación</p> <p>Tutela</p> <p>Dación de pago</p> <p>Suplantación</p> <p>Duplicidad de información</p> <p>Falta de autorización</p> <p>Sin vínculo con entidad</p> <p>Nunca ha tenido el producto</p> <p>No registra mora</p> <p>Calificación</p> <p>Otras variables</p> <p>Generar atribuciones especiales (Naturaleza del Reclamo), para los reclamos que exigen marcación en centrales de riesgo.</p> <p>Obligación al día</p> <p>Obligación a paz y salvo</p> <p>Desembargo cuenta</p> <p>Prescripción SU 082</p> <p>Prescripción T 284</p> <p>Permanencia de la información</p> <p>GMF (Gravamen de Movimiento Financiero) marcación y desmarcación</p>
--	--

	<p>Calificación</p> <p>Otras variables</p>
<i>Flujo Básico de Eventos</i>	<p>1. Identificar reportes que exigen la marcación de reclamos en las centrales de riesgo. Estos reportes deben tener un código de identificación que sea parametrizable e identificable según las políticas de la entidad financiera y la gestión de su sistema de reclamaciones.</p> <p>2. Una vez se identifican los reportes, se debe generar de forma manual o automática el archivo consolidado de reclamos para ser enviado al SARC.</p> <p>3. Tanto para la generación manual como para la automática, el sistema debe generar un archivo con los siguientes campos:</p> <p>Número de identificación, tipo de identificación, número de obligación, código del producto, tipo de transacción: (radicación ó Cierre), fecha de radicación, fecha de cierre, tipo de reclamo (actualización, corrección), subtipo de reclamo, naturaleza del reclamo, número de radicación del reclamo, código del mensaje (Reclamo en trámite, discusión judicial, orden judicial), Tipo de Respuesta (actualización, corrección, eliminación, ratificación y prórroga), campo de respuesta (para radicación va en blanco).</p>
<i>Flujo Alterno</i>	<p>2.1 Generación Automática del archivo de marcación: debe realizarse diariamente sólo para los reclamos que exigen las centrales de riesgo y agrupa todos los reclamos radicados y solucionados en el día, especificando la fecha de radicación o cierre del mismo. Los campos de los registros que componen el archivo, deben ser como mínimo los siguientes parámetros:</p> <p>Entidad que reporta: Número de secuencia, Tipo de registro, Nombre del archivo, Fecha de corte, Fecha generación del archivo y Total de registros.</p> <p>Información del reclamo: Tipo de Registro, tipo identificación, número identificación, número de crédito, número de obligación, código del producto, tipo de transacción, fecha de radicación, fecha de cierre, tipo de reclamo, subtipo de reclamo, naturaleza del reclamo, número de radicación, código del mensaje y tipo de</p>

	<p>respuesta.</p> <p>El archivo debe enviarse al sistema SARC implementado por la entidad.</p> <p>Para la generación manual del archivo, en el Sistema de Administración de reclamos, se debe tener un módulo de reportes que sea accesible por el usuario a través de una opción denominada 'Reportes Habeas Data' o cómo la entidad la desee identificar.</p> <p>Cuando un usuario ingrese a la opción de reportes Habeas Data y seleccione generar archivo de marcación para entidades de riesgo, debe ingresar los siguientes parámetros para generar el reporte:</p> <p>Rango de fechas para la generación del reporte (fecha de radicación y/o cierre del reclamo).</p> <p>Tipo de Transacción: Todas las opciones Radicación y cierre.</p> <p>Una vez se ingrese los parámetros, el usuario selecciona la opción de generar el archivo, el cual el sistema debe transmitir al sistema SARC de la entidad financiera para el posterior envío a las centrales de riesgo.</p>
<i>Poscondiciones</i>	<p>3.1 En caso de presentarse inconsistencias en la generación del archivo, (generación manual y generación automática), el sistema debe generar un Log de rechazos y enviarlo al analista del área de Control de Crédito encargado del proceso de marcación de reclamos en centrales de riesgo.</p>
<i>Frecuencia de ocurrencia</i>	<p>El reporte se debe generar diariamente.</p>
<i>Requerimientos especiales</i>	<p>Los campos solicitados en el archivo, son los necesarios para marcar en centrales de riesgo, se debe considerar que los campos solicitados por las centrales pueden variar y por tanto lo hace el archivo que se envía a SARC.</p> <p>Se debe realizar un acuerdo de servicio entre las áreas involucradas, Tecnología y Control de Crédito, para que ante un eventual inconveniente en el cargue automático del archivo de reclamos, como la caída del servidor del sistema de manejo de reclamaciones, el suceso sea informado por Tecnología a</p>

	Control de Crédito.
--	---------------------

Caso de Uso	CU - Transmitir archivos de marcación de reclamos a entidades de control
<i>Descripción</i>	El analista de Control de Crédito debe generar de forma diaria los archivos correspondientes a CIFIN y Datacrédito para la marcación (Radicación) y desmarque (Cierre) de los reclamos presentados en el día por los clientes del Banco.
<i>Precondiciones</i>	<p>Sistema de Gestión de Reclamos debe enviar diariamente el reporte de los reclamos radicados durante el día por los clientes, los campos que se envían en el reporte son necesarios para la generación de los dos archivos que se transmiten (archivo para CIFIN y archivo para Datacrédito).</p> <p>La composición de los campos que deben quedar reportados se relacionan en el caso de uso “Generar Archivo consolidado de reclamos”.</p>
<i>Flujo Básico de Eventos</i>	<p>1. El sistema SARC toma de manera automática los archivos de marcación generados de manera manual o automática por el sistema de gestión de reclamos de la entidad financiera (ver CU01) y almacena por número de radicación, el histórico de los reclamos generados. El archivo histórico de reclamos debe contener los siguientes campos:</p> <ul style="list-style-type: none"> • Número de identificación • Tipo de identificación • Número de crédito: Número de obligación. • Número de obligación SARC • Código del producto. • Tipo de transacción: Radicación, cierre • Fecha de radicación.

	<ul style="list-style-type: none"> • Fecha de cierre. • Tipo de reclamo: Actualización o corrección • Subtipo de reclamo • Naturaleza del reclamo • Número de radicación • Código para identificar los mensaje de Reclamo en trámite, discusión judicial u orden Judicial. • Tipo de respuesta (Actualización, corrección, eliminación, ratificación, prórroga). • Identificación del estado del reclamo (Reclamo cargado, reclamo sin NIT, reclamo sin número de obligación, reclamo radicado, reclamo cerrado y reclamo inconsistente).
	<p>2. El sistema debe validar que la obligación reportada desde el Sistema de Gestión de Reclamos de la entidad, exista en SARC.</p> <p>3. Luego de validar la obligación, se debe asignar automáticamente el número de obligación SARC vinculado al número de obligación que llega del aplicativo fuente.</p> <p>4. El sistema debe enviar para los tipos de transacción “Cierre”, el número de obligación con el que se radicó el reclamo en las Centrales de Riesgo. Para marcar la obligación cerrada correctamente, el sistema debe vincular en la tabla histórica del SARC el número de radicación del reclamo (el reclamo debe tener estado ‘Reclamo Radicado’) y solicitar que sea desmarcado con el numero de obligación SARC con el que se envió a marcación. Una vez el reclamo es cerrado debe cambiar el estado a ‘Enviado a desmarcar’.</p> <p>5. El Analista de Control y Crédito, debe ingresar a la funcionalidad definida en SARC para la generación de los archivos.</p> <p>6. El sistema presenta en la funcionalidad de generar archivo,</p>

	<p>presenta las siguientes opciones: Generar archivo Datacrédito y Generar archivo CIFIN.</p> <p>7. El Analista de Control y Crédito debe seleccionar una de las opciones de generación de archivo disponibles desde el sistema.</p> <p>8. El sistema debe generar el archivo seleccionado por el analista con la estructura definida por la central de riesgo.</p> <p>9. El sistema debe enviar el archivo a la central de riesgo correspondiente.</p>
<i>Flujo Alterno</i>	<p>3.1 Obligación no existe en el SARC.</p> <p>3.1.1 Si la obligación no existe en SARC y/o el reclamo está marcado como "Crédito no suministrado", el sistema debe asignar el número de obligación SARC de acuerdo a la siguiente lógica:</p> <p>Comparar por número de identificación en el SARC las obligaciones del cliente que presentó mora en los últimos doce (12) meses (parametrizables).</p> <p>Marcar aquellas obligaciones que presentaron mora mayor o igual a 30 días (parametrizables) en los últimos doce (12) meses (parametrizables).</p> <p>A la mora establecida de 30 días se le debe restar los parámetros de los productos definidos.</p> <p>De acuerdo a las condiciones anteriores se debe marcar la máxima última mora.</p> <p>Los últimos doce (12) meses se deben tomar como fecha menor o igual al último proceso reportado.</p> <p>3.1.2 Si el sistema al realizar el proceso no encuentra obligaciones con mora, debe marcar la obligación del cliente que presente mayor saldo a capital.</p> <p>3.1.3 El sistema debe asignar a cada reclamo un estado.</p> <p>Los reclamos cuyo número de identificación no existe en</p>

	<p>SARC, deben ser marcados como: Reclamo sin NIT.</p> <p>Los reclamos cuyo número de identificación existe en SARC, pero no posee obligaciones, debe marcarse como: Reclamo sin obligación.</p> <p>Los reclamos que se cargan en SARC con número de identificación y número de obligación, deben marcarse como: Reclamo cargado.</p> <p>Los reclamos que se generan y se envían en los archivos de Cifin y Datacrédito como tipo de transacción “Radicación”, deben marcarse como: Reclamo Radicado.</p> <p>Los reclamos que se generan y se envían en los archivos de Cifin y Datacrédito como tipo de transacción “Cierre”, deben marcarse como: Reclamo Cerrado.</p> <p>Los reclamos que al ser generados para las Centrales de Riesgo, presentaron inconsistencias en alguno de sus campos, deben marcarse como: Reclamo inconsistente.</p> <p>7.1 Ingresar la opción “Generar Archivo Datacrédito”</p> <p>7.1.1 El sistema debe generar el archivo para Datacrédito con la estructura definida por la central para la Formulación de Reclamos Genéricos Masivos.</p> <p>7.1.2 El sistema debe generar un archivo para Datacrédito con los reclamos marcados en la tabla histórica de SARC con estado “Reclamo Cargado”.</p> <p>7.1.3 El sistema debe asignar el número de obligación SARC en el campo correspondiente Número de Cuenta.</p> <p>7.2 Ingresar la opción “Generar Archivo CIFIN”</p> <p>7.2.1 El sistema debe generar el archivo para CIFIN con la estructura definida por la central para la Formulación de Reclamos Genéricos Masivos.</p> <p>7.2.2 El sistema debe generar archivo CIFIN los siguientes</p>
--	---

	<p>reclamos: Los reclamos marcados en la tabla histórica de reclamos de SARC con estado “Reclamo Cargado” y “Reclamo radicado” que tengan tipo de transacción “Cierre”.</p> <p>7.2.3 Asignar número de obligación SARC en el campo correspondiente Número de Cuenta.</p> <p>7.2.4 Se debe realizar las siguientes validaciones sobre los campos:</p> <p>Los campos marcados como opcionales no se transmiten, se debe dejar el campo con blancos (caracteres espacio).</p> <p>Cuando el tipo de transacción es “RADICACIÓN”, los campos correspondientes a “Número de radicación SIRE” [39], “Tipo de respuesta” y “Subtipo de respuesta” no deberán diligenciarse pero si respetar las longitudes definidas para estos.</p> <p>Cuando el tipo de transacción es “CIERRE”, los campos correspondientes a “Fecha de radicación entidad”, “Canal de radicación”, “Tipo del reclamo”, “Subtipo del reclamo”, “Código del mensaje” y “Naturaleza del reclamo” no deberán diligenciarse pero si respetar las longitudes definidas para estos.</p> <p>El campo código origen debe transmitirse como “RE: Radicado Entidad”.</p> <p>Tipo de transacción. Debe marcarse de acuerdo reporte enviado por el Sistema de Gestión de Reclamos.</p> <p>Fecha de Radicación debe corresponder a la fecha de radicación de la entidad.</p> <p>Canal de Radicación debe marcarse como “Presencial”.</p> <p>Tipo de Reclamo: Debe marcarse de acuerdo reporte enviado por Sistema de Gestión de Reclamos de la entidad.</p> <p>Subtipo de Reclamo: Debe marcarse de acuerdo reporte enviado por Sistema de Gestión de Reclamos de la</p>
--	--

	<p>entidad.</p> <p>Código de mensaje: Debe ir marcado como “Reclamo en trámite”.</p> <p>Naturaleza del reclamo: Debe marcarse de acuerdo reporte enviado por el Sistema de Gestión de Reclamos de la entidad.</p> <p>Tipo de respuesta: Debe marcarse de acuerdo reporte enviado por el Sistema de Gestión de Reclamos de la entidad.</p> <p>Paquete de información: Se debe homologar de acuerdo al tipo de reclamo que se relacione.</p> <p>Código de la sucursal: Indica el código de la sucursal asociada a la obligación</p>
<i>Poscondiciones</i>	Transmitir de manera encriptada los archivos a las centrales de riesgo.
<i>Frecuencia de ocurrencia</i>	Generación diaria.

3.5 VISTA DE ORGANIZACIONAL

3.5.1 Responsabilidades equipo de ejecución del proyecto

Para la ejecución de las actividades del proyecto, la entidad financiera debe contra con los siguientes roles y actividades genéricas.

Tabla 23: Matriz de responsabilidades

<i>Responsabilidad</i>	<i>Rol</i>	<i>Criterios de aceptación</i>
Definición del esquema de arquitectura	Director de Arquitectura	Visto bueno de arquitectura confirmado con la gerencia de TI y del proyecto.
Definición del esquema de Infraestructura	Director de Infraestructura	Visto bueno de la gerencia de TI y del proyecto
Definición y aceptación estructura y presupuesto del proyecto	Director de Vicepresidencia de Operaciones e Informática	Visto bueno de la presidencia, vicepresidencia de operaciones e informática y gerencia de TI
Definición organización proyecto	Director de Vicepresidencia de Operaciones e Informática	Visto bueno de la presidencia, vicepresidencia de operaciones e informática y gerencia de TI
Contratación	Gerente de Tecnología	Visto bueno de la vicepresidencia jurídica y la vicepresidencia de operaciones e informática
Documento con el resultado del GAP análisis.	Director de Vicepresidencia de Operaciones e Informática	Visto bueno de la vicepresidencia de operaciones e informática y gerencia de TI
Capacitación de la institución financiera en la herramienta	Director de Vicepresidencia de Operaciones e Informática	Visto bueno de la gerencia del proyecto y gerencia de TI
Definición del proveedor con el cual se negociará y realizará el GAP análisis.	Gerente de Tecnología	VoBo de la vicepresidencia de operaciones e informática

Matriz de proyectos y requerimientos	Director de Vicepresidencia de Operaciones e Informática	VoBo de las diferentes unidades de negocio , administrativas y operativas y la presidencia , la vicepresidencia de operaciones e informática y gerencia de TI
Elaboración del diccionario de Datos	Director de Vicepresidencia de Operaciones e Informática y equipo del Proyecto	VoBo de la gerencia de procesos y proyectos y tecnología.
Documentación de proceso y mapeo de servicios.	Director de Vicepresidencia de Operaciones e Informática y equipo del Proyecto	VoBo de la gerencia de procesos y proyectos y auditoría.

3.6 VISTA DE RECURSOS HUMANOS

3.6.1 Equipo para la ejecución de procesos

Según la definición de los procesos, es necesario contar con los siguientes roles:

Tabla 24: Roles requeridos para ejecución de procesos

<i>Rol</i>	<i>Criterios de aceptación</i>
Auxiliar Oficina	Captar solicitudes o reclamos basados en la ley de Habeas Data que los clientes generen en las oficinas
Administrador SARC	Parametrizar Sistema de Administración de Riesgo Crediticio (SARC) para el procesamiento y envío de reportes a las Centrales de Riesgo CIFI y Datacrédito.
Analista de Control y Crédito	Generación de archivos de pagos, incumplimientos de obligaciones de los clientes por mora y marcaciones.
Administrador sistema gestión de PQRS	Gestión de notificaciones para marcación de clientes en centrales de riesgo.

4 ARQUITECTURA DE INFORMACIÓN

La implementación de la ley Habeas Data requiere la integración de información con otros procesos de negocio para proveer un acceso consistente a todos los datos en la organización o aplicaciones que los requieran, sin restricciones de formato, fuente o localización de los mismos.

La integración de datos, puede requerir el desarrollo de nuevos adaptadores o motores de transformación que permitan la adecuación de la información de formato de dato a otro; pero cuando el concepto clave es SOA, la virtualización de los datos puede involucrar un desarrollo a nivel del Bus de Servicios Empresarial (ESB) para servicios genéricos que pueden ser consumidos por cualquier aplicación de la organización de manera que se puedan intercambiar datos sin importar su procedencia.

La vista de arquitectura de información tiene como objetivo definir el modelo canónico de datos, el ciclo de vida de información y la definición de flujos de mediación para servicios genéricos requeridos en la implementación de los procesos de la entidad financiera que cumpla con las definiciones de la Ley Habeas Data.

4.2 VISTAS DE ARQUITECTURA DE INFORMACIÓN

La representación de la arquitectura de información se efectuará haciendo uso de las siguientes vistas:

- **Vista Ciclo de Vida de la Información:** Permite identificar la temporalidad de la información relacionada con la duración que debe tener cada proceso según la disposición de la ley.
- **Vista de Modelado Canónico de Datos:** Es una definición de estructura de datos genérica e independiente de la plataforma de implementación, establecida por un patrón de diseño para la integración de aplicaciones.

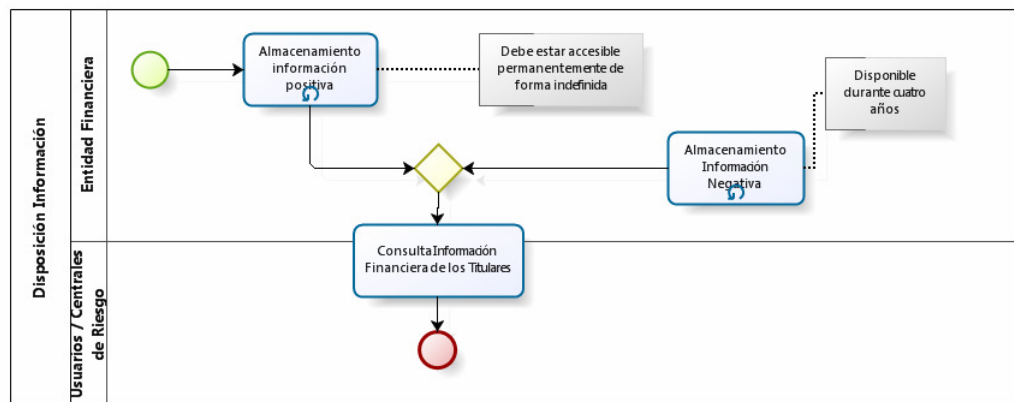
4.3 CICLO DE VIDA DE LA INFORMACIÓN

El ciclo de vida de la información permite establecer el eje horizontal que representa el tiempo desde su creación hasta su destrucción.

La importancia de establecer el ciclo de vida de la información es que ésta tiene valor de administración por procesamiento y almacenamiento, por lo cual es necesario determinar el tiempo exacto en que la organización requiere un registro, sujetándose a los niveles de servicio, los requerimientos legislativos, continuidad de negocio y oportunidades de mercado.

Dentro del marco arquitectónico para la implementación de la Ley Habeas Data, se establecen los ciclos de vida de la información relacionada a los macroprocesos que envuelve la ley: Gestión de consultas y reclamaciones, administración y circulación de información.

4.3.1 Ciclo de vida para macroproceso de Administración de la Información



powered by
Bizagi
Process Modeler

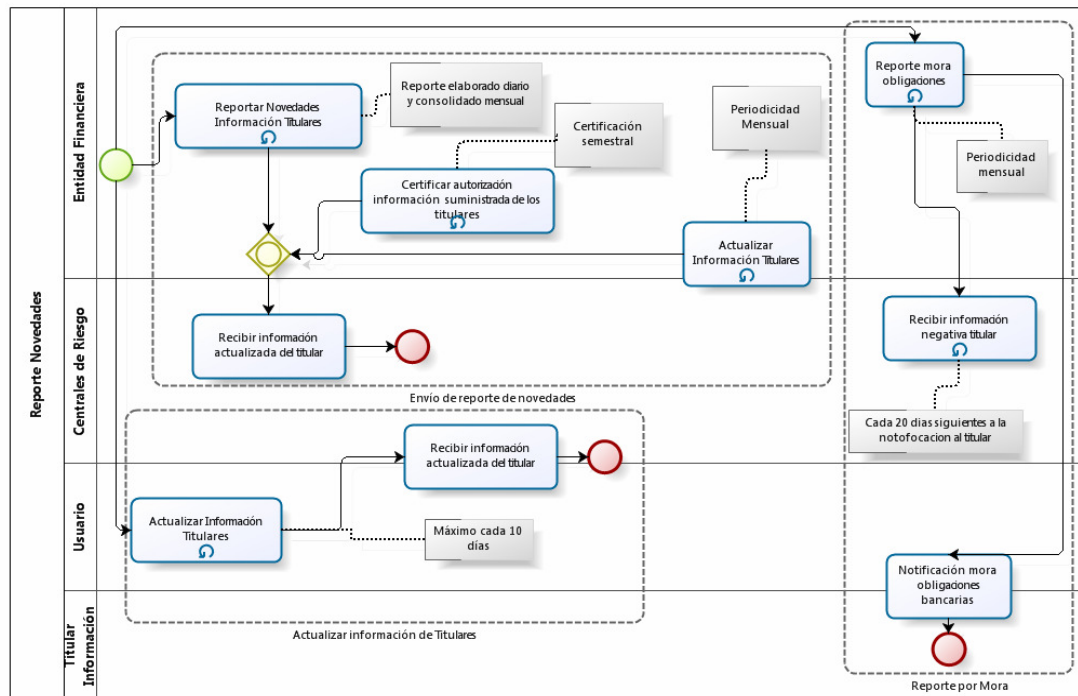
[Fuente: Propia]

Ilustración 12: Proceso de disposición de información

Según lo establecido en la ley, la información financiera positiva debe permanecer indefinidamente a disposición de los operadores y demás usuarios de la

información. Mientras la información financiera con reporte negativo solo permanece cuatro años en los bancos de datos de las fuentes de información. Ver gráfico para mayor claridad.

4.3.2 Ciclo de vida para macroproceso de Circulación de la Información



[Fuente: Propia]

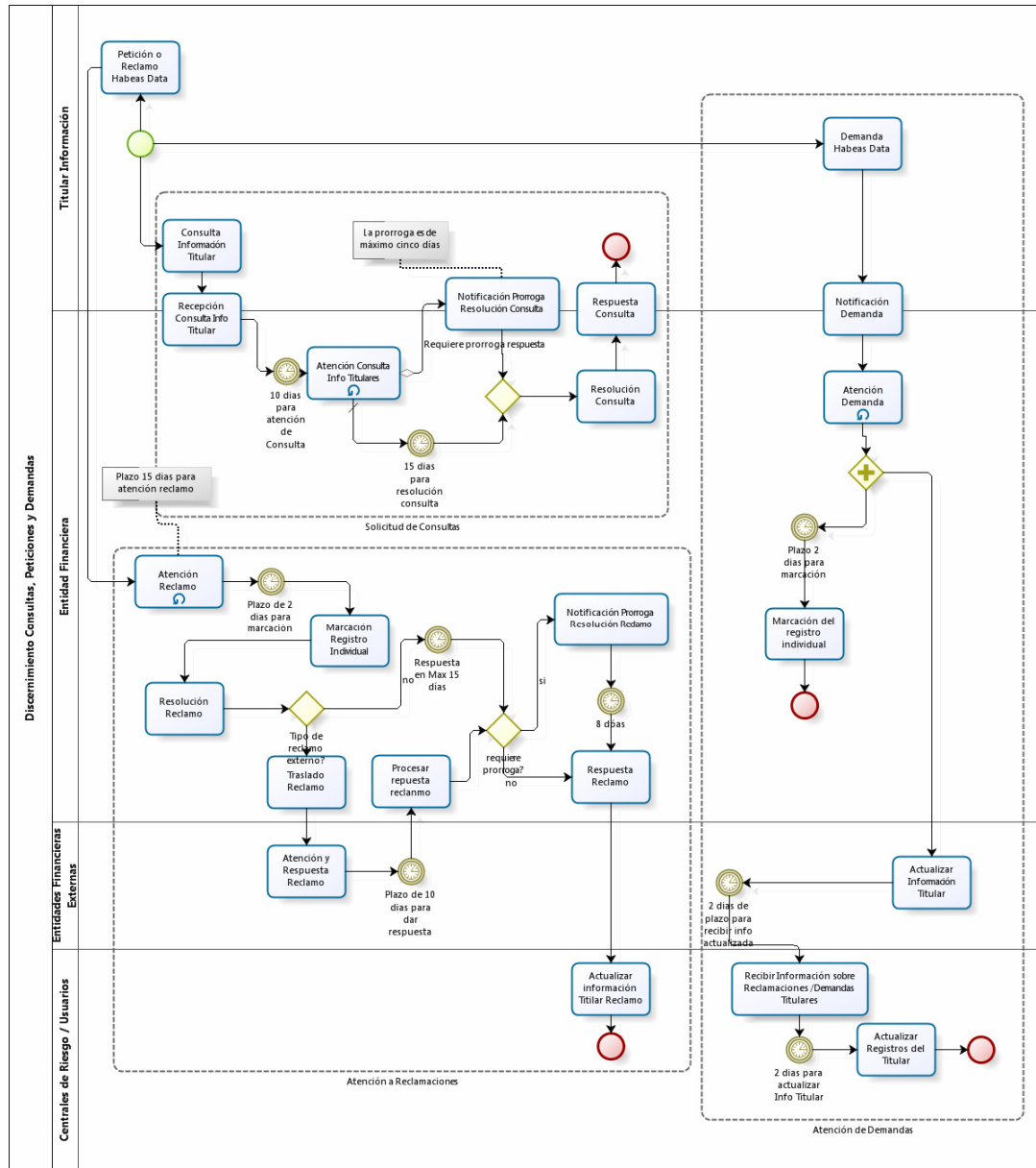
Ilustración 13: Proceso de reporte de novedades

Para el tratamiento de estos procesos originados por el titular y atendidos por las entidades financieras se delimita su periodicidad para asegurar un tiempo de respuesta oportuno y acorde con las protección de los derechos del titular de la información.

Cada proceso como consulta, reclamos, peticiones, y en ultima instancia, demandas, tienen una línea de atención diferente y diversos mecanismos internos para dar respuesta, pero cada fase del proceso es notificada y actualizada en los bancos de datos de los operadores, centrales de riesgo y demás usuarios autorizados de dicha información. Así, las entidades son autónomas para la resolución de los casos demandados por los titulares, pero estos obtendrán un tiempo de respuesta único sin importar el tipo de fuente de información a la cual fue impartida la solicitud.

En el diagrama se validan las diferentes actividades y las líneas de tiempo para la atención a los titulares, la inobservancia de estos periodos máximos para respuesta y notificaciones deriva en demandas y sanciones para las entidades que no cumplen con los plazos establecidos por la ley y acá especificados.

4.3.3 Ciclo de vida para macroproceso de Gestión de Consultas y Reclamaciones



[Fuente: Propia]

Ilustración 14: Macroproceso discernimiento PQRS

La especificación del parámetro de tiempo para cada uno de los procesos delimita el devenir de cada actividad y asegura el cumplimiento de las exigencias que en este sentido detalla la ley Habeas Data. Las notificaciones, el reporte del estado de las obligaciones y la actualización de la información tienen líneas de tiempo para su desarrollo y finalización. Así, tras el cumplimiento de los procesos en los periodos establecidos se determina el margen de acción del titular de la información para hacerle frente a diversas situaciones que requieren su intervención y manejo.

El ciclo de vida de la información inicia con el reporte de las novedades como se muestra en la ilustración 14. Corroborar la periodicidad establecida para cada proceso, los tiempos de respuesta entre las actividades y su sucesión lineal.

4.4 MODELO CANÓNICO DE DATOS

“En EAI (Enterprise Application Integration), el modelo canónico de datos es un patrón de diseño usado para comunicar entre diferentes formatos de datos. Esto introduce un formato adicional llamado *modelo canónico de datos*. En lugar de escribir adaptadores que permitan traducir entre todos y cada uno de los formatos, con el modelo canónico de datos solo es necesario traducir entre un formato y el formato canónico” [9]. Para la definición de la información involucrada dentro de los procesos relacionados con la ley de Habeas Data, se generará una propuesta de modelos de datos canónicos. Debido a que los servicios serán expuestos por el ESB por medio de Webservices, los datos de entrada y salida de los servicios serán especificados en un WSDL dividido por servicio. Las aplicaciones que requieran consumir estos servicios tendrán que estar en la capacidad de poder invocar dichos servicios e intercambiar la información en formato XML. La respuesta de los servicios en algunos casos puede ser un error, el cual puede ser funcional o técnico.

Por lo general, para SOA las estructuras canónicas se definen en esquemas XML, pero la definición de la estructura más conveniente se debe develar en los detalles de implementación generados por la entidad que utilice este modelo de referencia como punto de partida para la implementación de sus procesos. Por esto, en este marco se definirán los datos de entrada y salida de cada proceso, como se detallará a continuación.

4.4.1 Proceso: Comunicación a Clientes Morosos

Tabla 25: Tabla de atributos Registrar parámetros comunicado Habeas Data en SARC

Subproceso: Registrar parámetros comunicado Habeas Data en SARC			
Atributo	Tipo	Requerido	Descripción
Fecha Desde	Alfanumérico	Si	Fecha desde la cual se va a generar el reporte de clientes morosos.
Producto	Carácter	Si	Identificación del producto sobre el cual se realizará seguimiento de clientes en mora.
Días Mínimo	Numérico	Si	Días mínimos de mora que debe tener el cliente para que sea reportado.
Días Máximo	Numérico	Si	Días máximos de mora reportado.
Días Resta	Numérico	Si	Días que resta el cliente para la generación de sobregiro.
Comunicación Codeudores	Carácter	Si	Si se requiere notificación a codeudores
Mensaje comunicado	Alfanumérico	Si	Descripción del mensaje que debe recibir el cliente en mora.

Tabla 26: Tabla de atributos registrar población de clientes y/o codeudores morosos

Subproceso: Registrar población de clientes y/o codeudores morosos			
Atributo	Tipo	Requerido	Descripción

Numero de identificación	Alfanumérico	Si	Número de identificación del cliente en sobregiro
Tipo de identificación	Alfanumérico	Si	Reportar el tipo de identificación del cliente. N – NIT C – Cédula de Ciudadanía E – Cédula de Extranjería T – Tarjeta de Identidad P – Pasaporte S – Sociedad Publico- Privada F – Fideicomiso R – Registro Civil
Tipo persona	Alfanumérico	Si	PN – Persona natural PJ – Persona jurídica
Banca	Alfanumérico	Si	BI – Intermedia BT – Intermedia Centralizada BE – Empresarial BC – Corporativa BP – Personal BM – Masiva BD – Diplomática BO – Oficial BV – Vehículos
Nombre	Alfanumérico	Si	Nombre del Cliente

Sexo	Alfanumérico	Si	Sexo del Cliente M – Masculino F – Femenino E – Empresa
Fecha de nacimiento	Numérico	Si	Corresponde a la fecha de Nacimiento del cliente
Código de ciudad	Numérico	Si	Código de la ciudad del cliente.
Código departamento	Numérico	Si	Código del Departamento del cliente
Naturaleza	Numérico	Si	Naturaleza Jurídica asignada al Cliente: 0 – NO-APLICA-PERSONA NATURAL 1 – ENT-PUBLICA-NAL 2 – ENT-PUBLICA-DPTAL 3 – ENT-PUBLICA-MCPAL 4 – SOC-PRIVADA-EXTRJ 5 – SOC-PRIVADA-NAL 6 – SOCIEDAD-MULTNAL 7 – SOC-SIN-ANIMO-LCRO 8 – SOC-COOPERATIVA 9 – ENT-PUBLICA-EXTRJ 10-ENT- DE ECONOMIA MIXTA (GUBERNAMENTAL Y PRIVADA)
Fecha de constitución	Numérico	Si	Corresponde a la fecha de Constitución del cliente

Fecha de ingreso al banco	Numérico	Si	Corresponde a la fecha de ingreso a la institución financiera del cliente
Codigo ciu	Numérico	Si	Asignado al Cliente
Dpto correspondencia	Numérico	Si	Código del departamento de la dirección de correspondencia del cliente
Ciudad correspondencia	Numérico	Si	Código de la ciudad de la dirección de correspondencia del cliente.
Dirección correspondencia	Texto	Si	Corresponde a la dirección de correspondencia del cliente mas reciente.
Teléfono	Numérico	Si	Corresponde al número de teléfono del cliente (incluye el código del país e indicativo de la ciudad).
Celular	Numérico	Si	Corresponde al número celular del cliente (incluye el código del país).

Tabla 27: Tabla de atributos para la generación de población de clientes y/o codeudores morosos

Subproceso: Generar población de clientes y/o codeudores morosos			
Atributo	Tipo	Requerido	Descripción
Tipo de Novedad	Numérico	si	Se deben enviar los clientes nuevos del día y las actualizaciones que se presenten. 1.Cliente Nuevo 2.Actualización de cliente

Identificación Cliente	Texto	si	Identificación del cliente
Tipo de identificación cliente	Texto	Si	<p>Cuando el valor sea otros o ninguno de los anteriores enviar espacios en blanco.</p> <p>Para los registros de cédulas con dígito de chequeo se enviará tipo de identificación cédula de ciudadanía</p> <p>C - Cédula de Ciudadanía.</p> <p>N - Nit</p> <p>E - Cédula de Extranjería</p> <p>T - Tarjeta de Identidad</p> <p>P - Pasaporte</p> <p>D -Carné Diplomático</p> <p>S - Sociedad Extranjera sin Nit en Colombia</p> <p>F - Fideicomiso</p> <p>R - Registro Civil</p>
Tipo Persona	Texto	Si	<p>PN - Persona Natural</p> <p>PJ - Persona Jurídica</p>
Segmento Banca	Texto	Si	<p>BPN-B. Personal Pequeños negocios</p> <p>BP-B. Personal Privada</p> <p>BE-B. Empresarial</p> <p>BI-B Intermedia</p> <p>BI-B Intermedia Centralizada</p>

			BC Banca Corporativa BO-B. Oficial
Nombre cliente	Texto	Si	Nombre del Cliente
CIIU	Texto	si	Datos de CIIU para cada cliente de acuerdo a la tabla DANE. Ej. Para el caso de personas asalariadas el código es 0010.
STRCLISEXO	Texto	Si	Identificación del sexo del cliente. Para los clientes Persona Natural se recomienda manejar la nomenclatura M (masculino) y F (femenino). Para los clientes Persona Jurídica se les debe asignar E-Empresa si y sólo si su Tipo de Identificación es igual a NIT ó Sociedad Extranjera Sin NIT en Colombia ó Fideicomiso. M- Masculino F- Femenino E- Empresa
Fecha de Nacimiento	Numérico	Si	CRM no enviará las ciudades de nacimiento, si no se tiene la fecha de nacimiento se enviarán ceros.
Ciudad correspondencia	Numérico	Si	Se debe enviar dirección de todos los clientes tanto personas naturales como jurídicas. Para el caso de la ciudad del cliente, se debe llenar el campo con la dirección de envío de correspondencia.

Departamento correspondencia	Numérico	Si	Código Departamento asignado a la ciudad de envío de correspondencia.
Naturaleza cliente	Caracteres	Si	<p>CON: Consorcio / Unión Temporal</p> <p>EAT: Empresa Asociativa de Trabajo</p> <p>EPD: Entidad Pública Departamental</p> <p>EPM: Entidad Pública Municipal</p> <p>EPN: Entidad Pública Nacional</p> <p>LTD: Sociedad Limitada</p> <p>MX: Mixta</p> <p>OTR: Otra</p> <p>SAL: Entidad sin Animo de Lucro/Organización no gubernamental</p> <p>SAN: Sociedad Anónima</p> <p>SCA: Sociedad Comandita por Acción</p> <p>SCO: Entidad Cooperativa</p> <p>SCS: Sociedad Comandita Simple</p> <p>SDH: Empresa Unipersonal</p> <p>SMN: Sociedad Multinacional</p> <p>SPE: Sociedad Privada Extranjera</p> <p>SPN: Sociedad Privada Nacional</p>

			SPUE: Entidad Pública Extranjera Personas Naturales reportan naturaleza con un valor nulo.
Fecha de constitución	Fecha	Si	Fecha de Registro Cámara de Comercio. En los casos que este vacío se enviará en ceros.
Fecha vinculación	Numérico	Si	Fecha desde la cual es cliente Banco. Este campo aplica para persona natural y jurídica.
Departamento Correspondencia	Numérico	Si	Código del departamento de la dirección de correspondencia del cliente.
Ciudad Correspondencia	Numérico	Si	Código de la ciudad de la dirección de correspondencia del cliente.
Dirección Correspondencia	Texto	Si	Corresponde a la dirección de correspondencia del cliente mas reciente.

Tabla 28: Tabla de atributos para modificar registros al archivo de clientes y/o codeudores morosos

Subproceso: Modificar registros al archivo de clientes y/o codeudores morosos			
Atributo	Tipo	Requerido	Descripción
Mes Corte	Carácter	Si	Mes del archivo de clientes morosos a modificar.
Ruta Generación	Alfanumérico	Si	Ruta del archivo a modificar

4.4.2 Proceso: Generación diaria de archivos de pagos

Tabla 29: Tabla de atributos generar archivos de pagos e incumplidos

Subproceso: Generar archivos de pagos e incumplidos			
Atributo	Tipo	Requerido	Descripción
Fecha Inicial	Fecha	Si	Fecha de inicio para rango de generación de archivos.
Fecha Final	Fecha	Si	Fecha de final para rango de generación de archivos.

Criterios de salida:

Atributo	Tipo	Requerido	Descripción
Número de secuencia	Numérico	Si	Continuar con la secuencia, es decir, por cada línea o registro del archivo este campo se incrementa en 1.
Fecha de corte	Numérico	Si	Fecha de corte de la información
Fecha generación del archivo	Numérico	Si	Fecha en la cual se genera el archivo.
Total de registros	Numérico	Si	Número total de registros que se envían. Incluye todos los tipos de registros con sus respectivos totales de control
Tipo de novedad	Numérico	Si	Movimiento. Se coloca a cada uno de los registros que tienen movimiento.

Numero de identificacion	Alfanumérico	Si	Número de identificación del cliente deudor.
Tipo de identificación	Alfanumérico	Si	1 - Cédula de Ciudadanía 2 - Cédula de Extranjería 3 - Nit 4 - Tarjeta de Identidad 5 - Pasaporte 6 - Carne Diplomático 7 - Sociedad Extranjera sin Nit en Colombia. 8 - Fidecomiso. 9 - Registro Civil de Nacimiento.
Código oficina	Numérico	Si	Código de la oficina donde se encuentra radicada la obligación. Se debe reportar la Oficina equivalente en el estadístico, si se están realizando pruebas. Si la oficina no existe en el estadístico, se debe homologar a una oficina principal de acuerdo a la regional a la que pertenezca. Y si se homologa, se debe enviar como anexo al documento la tabla de conversión de las oficinas.
Número de obligación	Numérico	Si	Número de la tarjeta de crédito, incluye el prefijo.
Tipo de pago	Alfanumérico	Si	NR - Pago Normal CS - Castigo RT - Reestructurado CD - Condonado DP - Dación en Pago
Fecha de pago de la cuota	Numérico	Si	Es este campo se debe reportar la fecha en que el cliente realiza el pago de la cuota. Si el cliente efectúa varios pagos en el mes, se

			<p>debe reportar la fecha del último pago.</p> <p>Si es una reversión la fecha es la fecha en que se reversa el pago.</p>
Fecha último pago capital	Numérico	Si	Si el cliente presenta varios pagos durante el mes se debe enviar la fecha del último pago a capital. Si el último pago es reversado, esta fecha no se debe tener en cuenta.
Fecha último pago interés	Numérico	Si	Si el cliente presenta varios pagos durante el mes se debe enviar la fecha del último pago a interés. Si el último pago es reversado, esta fecha no se debe tener en cuenta.
Identificador	Alfanumérico	Si	<p>Identificador del campo “Valor Pago Capital”</p> <p>“-“ Para movimientos negativos. Cuando se ha reversado un pago.</p> <p>“+” Para movimientos positivos. Cuando el pago es aplicado correctamente.</p>
Valor pago capital	Numérico	Si	En esta casilla se debe reportar el valor a capital de los pagos realizados por el cliente en el mes. No debe llevar separador de decimales.
Valor pago interés cuentas por cobrar	Numérico	Si	En esta casilla se deben reportar los valores de los pagos de Intereses de Cuentas por Cobrar realizados por el cliente en el mes. No debe llevar separador de decimales.
Valor pago interés mora	Numérico	Si	En esta casilla se deben reportar el valor de los pagos de intereses de mora realizados por el cliente en el mes, contabilizados en la cuenta 16 y 64. No debe llevar separador de

			decimales.
Valor pago otros	Numérico	Si	En esta casilla se debe reportar los valores de los pagos correspondientes a seguros, comisiones, cuotas de manejo, etc. que el cliente ha realizado en el mes. No debe llevar separador de decimales.
Indicador moneda	Alfanumérico	Si	Indica el tipo de moneda con el cual se realiza el pago: C - Saldos de Credencial Ejecutiva (pesos) P - Saldos de tarjetas en pesos D - Saldos de tarjetas en dólares.
Sumatoria valor pago capital	Numérico	Si	Sumatoria del campo "Valor Pago Capital", No se debe utilizar separador de decimales.
Sumatoria valor pago interés cuentas por cobrar	Numérico	Si	Sumatoria del campo "Valor Pago Interés Cuentas por Cobrar". No se debe utilizar separador de decimales.
Sumatoria valor interés mora	Numérico	Si	Sumatoria del campo "Valor Interés Mora". No se debe utilizar separador de decimales.
Sumatoria valor otros	Numérico	Si	Sumatoria del campo "Valor Otros", No se debe utilizar separador de decimales.
Total de registros	Numérico	Si	Número total de registros tipo 5 enviados, incluye los registros de los totales de control.

Tabla 30: Tablar de atributos para parametrizar claves para cifrar archivos en SARC

Subproceso: Parametrizar claves para cifrar archivos en SARC			
Atributo	Tipo	Requerido	Descripción
Código Proceso	Numérico	Si	Identificación del proceso que debe parametrizarse
Nombre Archivo	Alfanumérico	Si	Nombre de archivo que se desea encriptar
Proveedor o Tercero	Carácter	Si	Código de tercero
Nombre Llave o Clave	Alfanumérico	Si	Clave de encriptación
Ubicación Llave o Clave	Alfanumérico	Si	Ubicación física de la clave de encriptación
Aplicación Para Encriptar	Alfanumérico	Si	Definición de la aplicación que se usa para encriptar.

4.4.3 Proceso: Novedades de los reportes a las centrales de riesgo

Tabla 31: Tabla de atributos para actualizar obligaciones de los reportes generados a las centrales de riesgo

Subproceso: Actualizar obligaciones de los reportes generados a las centrales de riesgo			
Atributo	Tipo	Requerido	Descripción
Tipo Reporte	Carácter	Si	Identificación de los reportes disponibles sobre el cual se desea generar una novedad, tales como: reporte mensual cartera total,

			reporte pagos cartera total, reporte mensual tarjeta de crédito Visa o MasterCard.
Plantilla	Carácter	Si	Lista de plantillas asociadas al reporte seleccionado.
Ubicación Archivo	Carácter	Si	Ruta de la ubicación física del archivo que contiene la información del reporte sobre el cual se quieren generar las novedades.
No Registro	Numérico	Si	Identificación del registro actualizado.
Campo	Carácter	Si	Identificación del campo actualizado.
Inconsistencia	Carácter	Si	Identificación de tipo de inconsistencia.

Tabla 32: Tabla de atributos para la consulta de reportes de las centrales de riesgo en SARC

Subproceso: Consultar reportes de las centrales de riesgo en SARC			
Atributo	Tipo	Requerido	Descripción
Tipo Reporte	Carácter	Si	Identifica el tipo de reporte: Mensual cartera total, pagos cartera total, reporte mensual tarjeta de crédito, reporte pagos tarjeta de crédito.
Identificación	Numérico	Si	Número de identificación del cliente por el cual se realizará la consulta.

Nombre Cliente	Carácter	Si	Nombre del cliente por el cual se realizará la consulta.
Obligación	Carácter	Si	Identificación de obligación o producto.

Parámetros de salida:

<i>Atributo</i>	<i>Tipo</i>	<i>Requerido</i>	<i>Descripción</i>
Tipo de identificación	Numérico	Si	<p>Cuando el valor sea otros o ninguno de los anteriores enviar espacios en blanco.</p> <p>Para los registros de cédulas con dígito de chequeo se enviará tipo de identificación cédula de ciudadanía</p> <p>C - Cédula de Ciudadanía. N - Nit E - Cédula de Extranjería T - Tarjeta de Identidad P - Pasaporte D -Carné Diplomático S - Sociedad Extranjera sin Nit en Colombia F - Fideicomiso R - Registro Civil</p>
Número de identificación	Numérico	Si	Identificación del cliente
Nombre tercero	Caracteres	Si	Nombre del cliente
Número de la obligación	Numérico	Si	Clase de tarjeta (Débito, Crédito Visa, Crédito Mastercard)

Código sucursal	Numérico	Si	Número de la sucursal en dónde se generó la obligación
Calidad	Alfanumérico	Si	Identificación de la calidad del tercero.
Calificación	Numérico	Si	Clasificación de segmento de banca.
Situación o estado del titular	Alfanumérico	Si	Descripción de la situación actual del titular. Ej: En proceso jurídico, en mora simple, sin obligaciones en mora, entre otros.
Estado	Numérico	Si	Estado de reclamos reportados a las centrales de riesgo
Tiempo de mora	Numérico	Si	Cantidad de días en las que se encuentra en mora una obligación financiera de un tercero.
Fecha de corte	Fecha	Si	Fecha de corte de pago ordinario de obligación financiera en estado de mora.
Fecha inicial o expedición	Fecha	Si	Fecha de expedición de la obligación.
Fecha terminación	Fecha	Si	Fecha de terminación de periodo de gracia.
Fecha de exigibilidad	Fecha	Si	Fecha de corte para realizar pagos según proceso jurídico.
Fecha de prescripción	Fecha	Si	Fecha en dónde se prescribe la obligación en mora.
Fecha de pago	Fecha	Si	Fecha del último pago realizado.
Modo extinción	Alfanumérico	Si	Modo de extinción comprometido con el deudor para el cumplimiento de la

			obligación.
Tipo de pago	Numérico	Si	NR - Pago Normal CS - Castigo RT - Reestructurado CD - Condonado DP - Dación en Pago
Periodicidad de pago	Numérico	Si	Cada cuanto tiempo se debe generar el pago: Anual, mensual, quincenal, semanal, diaria.
Probabilidad de no pago	Numérico	Si	Porcentaje de estudio de probabilidad de mora del cliente generada en estudio del crédito.
Número de cuotas pagadas	Numérico	Si	Cantidad de cuotas que el cliente ha cancelado de su obligación en mora.
Número de cuotas pactadas	Numérico	Si	Cantidad de cuotas pactadas en redefinición del pago para la obligación financiera en mora.
Cuotas en mora	Numérico	Si	Cantidad de cuotas atrasadas según el hábito de pago definido con el cliente.
Valor o cupo	Numérico	Si	Monto total de la obligación financiera.
Valor de mora	Numérico	Si	Sumatoria total del saldo en mora.
Valor del saldo	Numérico	Si	Sumatoria del total de la obligación financiera.
Valor de la cuota	Numérico	Si	Monto de la cuota de la obligación.
Valor de cargo fijo	Numérico	Si	Valor fijo de la obligación.
Línea de crédito	Alfanumérico	Si	Definición de la línea de crédito en la que se clasifica la

			obligación financiera.
Cláusula de permanencia	Alfanumérico	Si	Descripción de la cláusula de permanencia firmada por el cliente para la obligación financiera.
Tipo de contrato	Alfanumérico	Si	Descripción del tipo de contrato que respalda la obligación.
Estado de contrato	Alfanumérico	Si	Definición del estado en que se encuentra el contrato que respalda la obligación financiera.
Termino o vigencia del contrato	Fecha	Si	Fecha de vencimiento del contrato.
Numero de meses del contrato	Numérico	Si	Número meses que cubre el contrato.
Naturaleza jurídica	Alfanumérico	Si	<p>Naturaleza Jurídica asignada al Cliente:</p> <p>0 – NO-APLICA-PERSONA NATURAL</p> <p>1 – ENT-PUBLICA-NAL</p> <p>2 – ENT-PUBLICA-DPTAL</p> <p>3 – ENT-PUBLICA-MCPAL</p> <p>4 – SOC-PRIVADA-EXTRJ</p> <p>5 – SOC-PRIVADA-NAL</p> <p>6 – SOCIEDAD-MULTNAL</p> <p>7 – SOC-SIN-ANIMO-LCRO</p> <p>8 – SOC-COOPERATIVA</p> <p>9 – ENT-PUBLICA-EXTRJ</p> <p>10-ENT- DE ECONOMIA MIXTA (GUBERNAMENTAL Y</p>

			PRIVADA)
Modalidad de crédito	Numérico	Si	Modalidad en la que se encuentra el crédito según la clasificación de la entidad financiera.
Tipo de moneda	Numérico	Si	Moneda con la que se genera la pago y desembolso de la obligación.
Tipo de garantía	Numérico	Si	Tipo de garantía que cubre la obligación en mora.
Valor de la garantía	Numérico	Si	Monto de la garantía.
Obligación reestructurada	Alfanumérico	Si	Reestructuración financiera de la obligación en mora.
Naturaleza de la reestructuración	Numérico	Si	Nueva clasificación de la naturaleza según la reestructuración.
Número de reestructuraciones	Numérico	Si	Cantidad de reestructuraciones de pago a las que se ha sometido la obligación financiera.
Clase tarjeta	Numérico	Si	Tipo de tarjeta con la que se genera la obligación financiera.
No de cheques devueltos	Numérico	Si	Cantidad de cheques devueltos por sobregiros u otros eventos.
Plazo	Alfanumérico	Si	Plazo generado para el cliente.
Días de cartera	Numérico	Si	Cantidad de días en la que la obligación se encuentra en cartera.
Tipo de cuenta	Numérico	Si	Tipo de cuenta en la que se clasifica la obligación financiera del cliente.

Cupo sobregiro	Numérico	Si	Cupo que se encuentra en sobregiro.
Días autorizados	Numérico	Si	Cantidad de días de autorizados de espera para que el cliente ponga sus obligaciones al día.
Dirección residencia del tercero	Alfanumérico	Si	Corresponde a la dirección de correspondencia del cliente mas reciente.
Teléfono residencia del tercero	Alfanumérico	Si	Corresponde al número de teléfono del cliente (incluye el código del país e indicativo de la ciudad).
Ciudad residencia del tercero	Numérico	Si	Código de la ciudad de de la dirección de correspondencia del tercero.
Código departamento residencia.	Numérico	Si	Código del departamento de la dirección de correspondencia del tercero.
Nombre empresa	Alfanumérico	Si	Nombre de la empresa.
Dirección de la empresa	Alfanumérico	Si	Corresponde a la dirección de correspondencia de la empresa mas reciente.
Teléfono de la empresa	Alfanumérico	Si	Corresponde al número de teléfono de la empresa (incluye el código del país e indicativo de la ciudad).
Código ciudad empresa	Numérico	Si	Código de la ciudad de de la dirección de correspondencia de la empresa
Departamento empresa del tercero	Numérico	Si	Código del departamento de la dirección de correspondencia de la empresa.
Fecha inicio	Fecha	Si	Fecha en la que inicia la exención del Gravamen de

exención GMF			Movimiento Financiero.
Fecha terminación exención GMF	Fecha	Si	Fecha en la que finaliza la exención del Gravamen de Movimiento Financiero.
Número de renovación CDT	Numérico	Si	Código con la que se genera la renovación de un producto CDT.
Cuenta ahorro exenta GMF	Numérico	Si	Número de cuenta exenta del gravamen de movimiento financiero.
Tipo de identificación originaria	Numérico	Si	<p>Tipo de identificación de fiduciante.</p> <p>C - Cédula de Ciudadanía.</p> <p>N - Nit</p> <p>E - Cédula de Extranjería</p> <p>T - Tarjeta de Identidad</p> <p>P - Pasaporte</p> <p>D -Carné Diplomático</p> <p>S - Sociedad Extranjera sin Nit en Colombia</p> <p>F - Fideicomiso</p> <p>R - Registro Civil</p>
Número de identificación originaria	Numérico	Si	Número de identificación del fiduciante.
Tipo de entidad originaria	Numérico	Si	Descripción de la entidad a la que pertenece el fiduciante en caso de ser persona jurídica.
Código de entidad	Numérico	Si	Número único de identificación

originaria			del tipo de empresa según el código SIIU.
Tipo de fideicomiso	Numérico	Si	Clasificación del fideicomiso: 01 - Fideicomisos de inversión 02 - Fideicomisos de garantía 03-Fideicomisos de administración y mixtos.
Número del fideicomiso	Numérico	Si	Identificación única del fideicomiso.
Nombre fideicomiso	Alfanumérico	Si	Nombre legal del fideicomiso.
Tipo de deuda cartera	Numérico	Si	Clasificación de la deuda en el sistema de cartera.
Tipo de póliza	Alfanumérico	Si	Tipo de póliza que cubre la obligación en mora.
Código de ramo	Numérico	Si	Número de identificación única de un ramo de negocio.
Fecha última modificación	Fecha	Si	Fecha de la última modificación realizada sobre la obligación financiera.
Tipo novedad	Numérico	Si	Tipo de novedad aplicada a la obligación financiera.

4.4.4 Proceso: Marcación de reclamos en las centrales de riesgo

Tabla 33: Tabla de atributos para la generación de archivo consolidado de reclamos

Subproceso: Generar archivo consolidado de reclamos		
Entidad	Atributo	Tipo
Reclamos: Almacena la información de los reclamos radicados o cerrados durante el día y que deben ser enviados para marcación y desmarcación a centrales de riesgo.	Tipo de registro	Numérico
	Tipo de Identificación	Alfanumérico
	Numero de Identificación	Alfanumérico
	Número de Crédito: Número de Obligación	Numérico
	Código del producto	Numérico
	Tipo de Transacción	Numérico
	Fecha de radicación	Fecha
	Fecha de cierre	Fecha
	Tipo de Reclamo	Numérico
	Subtipo de Reclamo	Numérico
	Naturaleza del Reclamo	Numérico
	Número de radicación	Numérico
	Código del mensaje	Numérico
	Tipo de respuesta	Numérico
Entidad	Descripción	Tipo

Estado Reclamo: Almacena los posibles estados de los reclamos.	Código del estado	Numérico
	Descripción del Estado.	Alfanumérico

Entidad	Atributo	Tipo
Reclamos diarios: Almacena temporalmente los reclamos diarios enviados por cada cliente.	Tipo de registro	Numérico
	Tipo de Identificación	Alfanumérico
	Numero de Identificación	Alfanumérico
	Número de Crédito: Número de Obligación	Numérico
	Código del producto	Numérico
	Tipo de Transacción	Numérico
	Fecha de radicación	Fecha
	Fecha de cierre	Fecha
	Tipo de Reclamo	Numérico
	Sub tipo de Reclamo	Numérico
	Naturaleza del Reclamo	Numérico
	Estado de reclamos reportados a las centrales de riesgo	Numérico

Entidad	Atributo	Tipo
Reclamos inconsistencias:	Tipoidentificacion	Alfanumérico

	Numidentificacion	Alfanumérico
	Numcredito	Numérico
	Codproducto	Numérico
	Numtipotransaccion	Numérico
	Fecradicacion	Fecha
	Feccierre	Fecha
	Numtiporeclamo	Numérico
	Subtiporeclamo	Numérico
	Naturalezareclamo	Numérico
	Numradicacion	Numérico
	Codmensaje	Numérico
	Numtiporespuesta	Numérico
	Estado	Numérico
	Consistencia	Alfanumérico

5 ARQUITECTURA DE SERVICIOS

La estructura arquitectónica para la implementación de la Ley Habeas Data en el sector financiero, al ser un marco de referencia de industria, define los servicios pero no establece detalles de flujos de medición e implementación de los servicios dentro de una infraestructura determinada porque cada entidad diverge el despliegue de su plataforma de tecnología.

5.2 OBJETIVOS DE LA ARQUITECTURA DE SERVICIOS

El modelado del Servicio es el corazón de la **Arquitectura Orientada a Servicios (SOA)**.

El Modelo de Servicio permite generar la identificación y especificación de los servicios, así como la toma de decisiones que es necesario para la realización de servicios de apoyo. Bajo la metodología de RUP/SOMA el modelado de servicio se compone de varias secciones cada una de las cuales tiene un objetivo de especificación, resumido en los siguientes ítems:

- Identificar los servicios candidatos y tomar las decisiones acerca de los servicios que realmente estarán expuestos.
- Especificar el contrato entre el proveedor de servicios y el consumidor de los servicios.
- Servicios asociados con los componentes necesarios para la realización de estos servicios.

5.3 PORTAFOLIO DE SERVICIOS

El portafolio de servicios es una estructura simple que permite categorizar jerárquicamente los servicios. Este sistema de clasificación según la metodología RUP/SOMA, se basa en áreas funcionales del proceso que se va a implementar.

El portafolio de servicios debe contener una cantidad administrable de servicios candidatos, los cuales se asocien a los objetivos del negocio.

5.3.1 Servicios

- 1 Proceso Habeas Data
 - 1.1 Reclamaciones
 - 1.2 Reporte de novedades
 - 1.1.1 Reportar novedades información titulares
 - 1.1.2 Reporte de Obligaciones en Mora
 - 1.1.3 Actualizar Información de los Titulares
 - 1.2.1 Consulta Información Titular
 - 1.2.2 Reclamo Habeas Data
 - 1.2.3 Demanda Habeas Data
 - 1.1.1.1 Certificar autorización Titulares

- 1.1.1.2 Actualizar información Titulares
- 1.1.1.3 Enviar información actualizada Titular
- 1.1.2.1 Notificación de mora en obligaciones
- 1.1.2.2 Procesar respuesta a notificación de mora
- 1.1.2.3 Enviar información negativa del Titular
- 1.1.3.1 Enviar información actualizada del titular
- 1.2.1.1 Recepción Consulta información titular
- 1.2.1.2 Atención Consulta Información titular
- 1.2.1.3 Notificación de prórroga
- 1.2.1.4 Resolución de Consulta
- 1.2.1.5. Respuesta de Consulta
- 1.2.2.1 Atención de Reclamo
- 1.2.2.2 Marcación de registro individual
- 1.2.2.3 Resolución de reclamo
- 1.2.2.4 Procesar respuesta reclamo
- 1.2.2.5 Notificación de prórroga

- 1.2.2.6 Enviar respuesta de reclamo
- 1.2.2.7 Actualizar información titular reclamación
- 1.2.3.1 Recibir información demanda Habeas Data
- 1.2.3.1 Recibir demanda Habeas Data
- 1.2.3.2 Notificar Demanda
- 1.2.3.3 Marcación de registro individual con demanda
- 1.2.3.4 Solicitar actualización información demanda

5.3.2 Jerarquía de Servicios

Categoría: Gestión de Información

- 1.1 Administración y circulación de información
- 1.1.1 Reportar novedades información titulares
- 1.1.1.1 Certificar autorización Titulares
- 1.1.1.2 Enviar información actualizada Titular
- 1.1.2 Reporte de Obligaciones en Mora
- 1.1.2.1 Notificación de mora en obligaciones

- 1.1.2.2 Procesar respuesta a notificación de mora
- 1.1.2.3 Enviar información negativa del Titular

Categoría: Discernimiento consultas, peticiones y demandas

- 1.2 Reclamaciones
 - 1.2.1 Consulta Información Titular
 - 1.2.1.1 Recepción Consulta información titular
 - 1.2.1.2 Atención Consulta Información titular
 - 1.2.1.3 Notificación de prorroga
 - 1.2.1.4 Resolución de Consulta
 - 1.2.1.5. Respuesta de Consulta
 - 1.2.2 Reclamo Habeas Data
 - 1.2.2.1 Atención de Reclamo
 - 1.2.2.2 Marcación de registro individual
 - 1.2.2.3 Resolución de reclamo
 - 1.2.2.4 Procesar respuesta reclamo
 - 1.2.2.5 Notificación de prorroga

- 1.2.2.6 Enviar respuesta de reclamo
- 1.2.2.7 Actualizar información titular reclamación
- 1.2.3 Demanda Habeas Data
 - 1.2.3.1 Recibir información demanda Habeas Data
 - 1.2.3.1 Recibir demanda Habeas Data
 - 1.2.3.2 Notificar Demanda
 - 1.2.3.3 Marcación de registro individual con demanda
 - 1.2.3.4 Solicitar actualización información demanda

Tabla 34: Tabla de clasificación de servicios

Servicio	Descripción	Estado	Asociaciones	
			Proceso	Meta
Administración y circulación de información	Servicio permitirá generar el flujo de información dentro del proceso para cumplir con acuerdos de servicio Habeas Data.	C	Gestión de Información	Implementar las políticas de gestión de información
Reportar novedades información titulares	Servicio que permite a la entidad financiera generar reportes a las centrales de riesgo para la actualización de información.	E	Gestión de Información	Enviar reportes de novedades referentes a procesos generados por el cliente.

Certificar autorización Titulares	Servicio por medio del cual la entidad financiera puede validar la autorización de los titulares de información para la gestión y uso de sus datos.	C	Gestión de Información	Asegurar la autorización del cliente para el manejo de su información.
Enviar información actualizada Titular	Servicio que permite enviar a las centrales de riesgo CIFIN y Datacrédito los reportes de actualización de	E	Gestión de Información	Reportar actualizaciones de datos de los clientes
Reporte de Obligaciones en Mora	Servicio que permite que las entidades financieras generar un reporte de información negativa de un titular por mora en sus obligaciones financieras.	E	Gestión de Información	Generar reporte de obligaciones en mora.
Notificación de mora en obligaciones	Servicio que permite generar comunicado al cliente para informar que tiene obligaciones financieras en mora que serán reportadas a las centrales de riesgo.	E	Gestión de Información	Enviar comunicado de notificación de reporte en centrales de riesgo a cliente en mora.
Procesar respuesta a notificación de mora	Servicio que permite procesar las respuestas de aceptación o rechazo de reporte por parte de los clientes.	E	Gestión de Información	Recibir y procesar la respuesta del cliente respecto a notificación de mora.
Enviar información negativa del	Servicio que permite generar archivos de marcación y enviar información negativa	E	Gestión de Información	Generar y enviar archivo de marcación por mora en

Titular	del titular a centrales de riesgo.			obligaciones.
Reclamaciones	Servicio que permite el procesamiento de las reclamaciones registradas por personas naturales o jurídicas en la entidad financiera.	C	Consultas, peticiones y demandas	Procesar reclamaciones o peticiones basadas en la ley de Habeas Data registradas en la entidad financieras.
Consulta información Titular	Servicio que permite generar el flujo de procesamiento desde la recepción hasta la respuesta de la solicitud de una consulta individual de información.	C	Consultas, peticiones y demandas	Procesamiento de solicitudes de consulta.
Recepción Consulta información titular	Servicio que permite a persona natural o jurídica generar una consulta sobre la información que sobre ella reposa en las centrales de riesgo.	E	Consultas, peticiones y demandas	Registrar solicitud de consulta de registro individual.
Atención Consulta Información titular	Servicio que permite validar el tipo de solicitud de consulta para validar cual es el entre que debe encargarse de generar su solución y asignársela.	E	Consultas, peticiones y demandas	Asignación de caso de solicitud de consulta.
Notificación de prorroga	Servicio para generar comunicado de notificación de prorroga en la atención de la solicitud de consulta a cliente.	E	Consultas, peticiones y demandas	Generar notificación de prorroga en envío de respuesta.

Resolución de Consulta	Servicio para que el área solucionadora registre el resultado de la consulta solicitada por el cliente.	E	Consultas, peticiones y demandas	Registrar respuesta a caso de solicitud de consulta.
Respuesta de Consulta	Servicio para el envío de comunicado a solicitante con respuesta de consulta por registro individual.	E	Consultas, peticiones y demandas	Generar envío de respuesta de consulta a persona radicadora.
Reclamo Habeas Data	Servicio que permita a persona natural o jurídica registrar una reclamación en entidad financiera.	E	Consultas, peticiones y demandas	Registrar reclamación en entidad.
Atención de Reclamo	Servicio que permite validar la naturaleza del reclamo y escalar a área solucionadora.	E	Consultas, peticiones y demandas	Asignar caso de reclamación a área o funcionario asignado.
Marcación de registro individual	Servicio que permite enviar marcación de registro individual con la leyenda 'Proceso de reclamación' a centrales de riesgo.	E	Consultas, peticiones y demandas	Enviar marcación de registro a centrales de riesgo.
Resolución de reclamo	Servicio que le permite al área solucionadora realizar el procedimiento de atención a reclamo.	C	Consultas, peticiones y demandas	Realizar proceso de atención de reclamo para su solución.
Procesar respuesta reclamo	Servicio que permite al área solucionadora registrar la respuesta de la reclamación registrada.	E	Consultas, peticiones y demandas	Registrar respuesta a reclamo.
Enviar respuesta de	Servicio para generar respuesta de solución	E	Consultas, peticiones y	Enviar respuesta

reclamo	de reclamación a persona radicadora.		demandas	a reclamación.
Actualizar información titular reclamación	Servicio que permite a la entidad financiera realizar marcación de registros a las centrales de riesgo según resultado de gestión de reclamaciones.	E	Consultas, peticiones y demandas	Actualizar información de registros individuales a centrales de riesgo.
Demanda Habeas Data	Servicio para la gestión de procesos de demanda instaurados por personas naturales o jurídicas.	C	Consultas, peticiones y demandas	Gestionar demandas Habeas Data.
Recibir información demanda Habeas Data	Servicio que permite a la entidad financiera conocer que existe un proceso de demanda vigente para algún titular de información.	E	Consultas, peticiones y demandas	Actualizar información de demandas sobre titulares de manejo por la entidad financiera.
Recibir demanda Habeas Data	Servicio que permite el ingreso de la demanda Habeas Data en la entidad financiera.	E	Consultas, peticiones y demandas	Registrar demanda.
Marcación de registro individual con demanda	Servicio que permite notificar la demanda a centrales de riesgo cuando dicha demanda compete a entidad financiera.	E	Consultas, peticiones y demandas	Marcación del registro individual por concepto de demanda.
Solicitar actualización información demanda	Servicio que permite a la entidad financiera solicitar actualización de la demanda en proceso.	E	Consultas, peticiones y demandas	Solicitud actualización de información sobre demanda a terceros.

Estado: “C” de Servicio Candidato, “E” de Servicio Expuesto.

Tabla 35: Flujo de mensajes entre servicios

Servicio	Operación	Mensaje de entrada	Mensaje de Salida	Excepción
Reportar novedades información titulares	Enviar reportes de novedades referentes a procesos generados por el cliente.	Estado de procesos de reclamación o demandas	Archivos de novedades para CIFIN y Datacrédito.	Generación incorrecta de archivos.
Certificar autorización Titulares	Asegurar la autorización del cliente para el manejo de su información.	Información del cliente.	Identificación de cliente, productos, fecha de autorización, estado de autorización.	Cliente inexistente.
Enviar información actualizada Titular	Reportar actualizaciones de datos de los clientes	Archivos de novedades para CIFIN y Datacrédito.	Log de resultado de la operación	Archivo de novedad no enviado por falla en formato o contenido.
Reporte de Obligaciones en Mora	Generar reporte de obligaciones en mora.	Información de compensación de pagos para todos los productos que se reportan a las centrales de riesgo.	Archivos de novedades de clientes en mora.	Datos de archivo de clientes en mora incorrectos.
Notificación de mora en obligaciones	Enviar comunicado de notificación de reporte en centrales de	Registro unificado de cliente en mora.	Extracto bancario con anotación de reporte a Centrales de	Identificación del cliente inexistente. Falla en generación de

	riesgo a cliente en mora.		riesgo por mora en obligaciones financieras.	extracto.
Procesar respuesta a notificación de mora	Recibir y procesar la respuesta del cliente respecto a notificación de mora.	Identificación de cliente, servicio en mora y fecha de notificación.	Relación de Identificación del cliente con reclamaciones en curso por servicio en mora.	Datos inconsistentes. Compensación de información reclamaciones vs notificaciones desajustada.
Enviar información negativa del Titular	Generar y enviar archivo de marcación por mora en obligaciones.	Archivo de reporte de clientes en mora para centrales de riesgo.	Log de respuesta de envío de archivo.	Archivo rechazado por información o formato inconsistente.
Identificación de cliente	productos	fecha de autorización	estado de autorización.	Identificación de cliente
Consulta información Titular	Procesamiento de solicitudes de consulta.	Identificación del titular, naturaleza de consulta y fecha de radicación.	Archivo de respuesta de consulta.	Datos incompletos.
Recepción Consulta información titular	Registrar solicitud de consulta de registro individual.	Identificación del titular, naturaleza de consulta y fecha de radicación.	Número de radicación de solicitud de consulta y datos asociados al registro.	Datos incompletos.
Atención Consulta Información titular	Asignación de caso de solicitud de consulta.	Número de radicación de solicitud de consulta y datos asociados al registro.	Identificación de área o funcionario asignado, fecha de asignación.	Notificación de asignación fallida.
Notificación	Generar	Número de	Archivo de	Dirección de

de prorroga	notificación de prorroga en envío de respuesta.	radicación de la solicitud, fecha de radicación, estado del proceso.	notificación, dirección de correspondencia cliente.	correspondencia cliente no conocida por el sistema. Datos incompletos.
Resolución de Consulta	Registrar respuesta a caso de solicitud de consulta.	No radicación de solicitud, No de radicación asignación.	Estado de la consulta, respuesta asociada.	Respuesta incoherente.
Respuesta de Consulta	Generar envío de respuesta de consulta a persona radicadora.	No radicación de solicitud, Información de solicitante y respuesta asociada a solicitud.	Archivo de respuesta a consulta de registro individual.	Falla en generación de archivo.
Reclamo Habeas Data	Registrar reclamación en entidad.	Identificación, nombre, tipo de reclamo, descripción del reclamo.	Número de radicación, fecha de radicación del reclamo.	Información incompleta en el registro de la reclamación.
Atención de Reclamo	Asignar caso de reclamación a área o funcionario asignado.	Número de radicación reclamo y datos asociados al registro.	Identificación de área o funcionario asignado, fecha de asignación.	Notificación de asignación fallida.
Marcación de registro individual	Enviar marcación de registro a centrales de riesgo.	Archivo de marcación de registro individual para las centrales de riesgo: Identificación de la persona, leyenda de 'reclamo en	Log de resultado del envío del archivo: Hora de la transacción, descripción del resultado, identificación del origen y destino.	Caída del canal en envío del archivo. Archivo inconsistente por estructura o contenido.

		proceso'		
Resolución de reclamo	Realizar proceso de atención de reclamo para su solución.	Número de radicación de solicitud de reclamo y datos asociados al registro.	Identificación de área o funcionario asignado, fecha de asignación.	Notificación de asignación fallida.
Procesar respuesta reclamo	Registrar respuesta a reclamo.	No radicación reclamo, tipo de reclamo, identificación de área solucionadora, Fecha de ingreso y asignación de registro.	Estado de reclamo, fecha de procesamiento, identificación de procesamiento externo, fecha de envío externo, log de gestión del requerimiento.	Información incompleta.
Enviar respuesta de reclamo	Enviar respuesta a reclamación.	Generar archivo de respuesta.	Generar log de archivo de respuesta.	Falla de canal.
Actualizar información titular reclamación	Actualizar información de registros individuales a centrales de riesgo.	Generar archivo de generación actualización de información en centrales de riesgo.	Log de transacciones de transferencia de archivo a centrales de riesgo.	Falla de canal. Archivo con fallas por formato o datos.
Demanda Habeas Data	Gestionar demandas Habeas Data.	Registro de demandas en proceso ante cualquier ente.	Archivo de actualización de datos.	
Recibir información demanda	Actualizar información de demandas sobre titulares	Recibir archivo consolidado de demandas	Log de actualización de registro en bases de datos	Falla por compensación de datos.

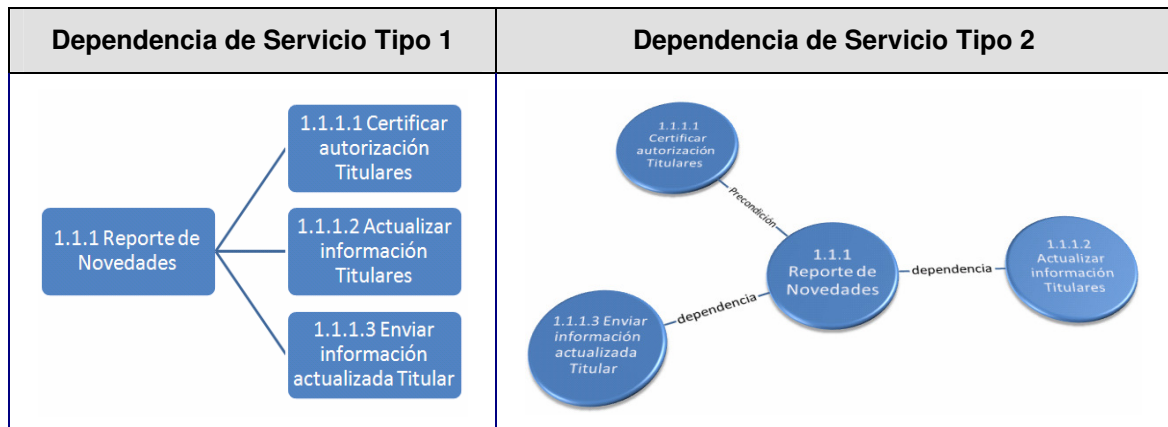
Habeas Data	de manejo por la entidad financiera.	en curso asociadas a titulares de información por Habeas Data.	interna de la entidad.	Caida del canal de comunicaciones.
Recibir demanda Habeas Data	Registrar demanda.	Información de titular, tipo de demanda, información del demandado, fechas de radicación.	No de radicación de demanda, definición de relación con la entidad.	Información incompleta.
Marcación de registro individual con demanda	Marcación de registro individual por concepto de demanda.	Archivo de marcación de registro individual, información de titular, fecha de demanda, leyenda de marcación.	Log de transferencia de archivo a central de riesgo.	Falla del canal, archivo inconsistente por formato o datos.
Solicitar actualización información demanda	Solicitud actualización de información sobre demanda a terceros.	Registro de solicitud con rango de fechas para actualización de información.	Archivo de actualización de registro de estado de demandas a titulares. Información de titular, tipo de demanda, información del demandado, fechas de radicación.	Falla en el canal. Inconsistencia el en el registro por compensación de datos o formato de interfaz.

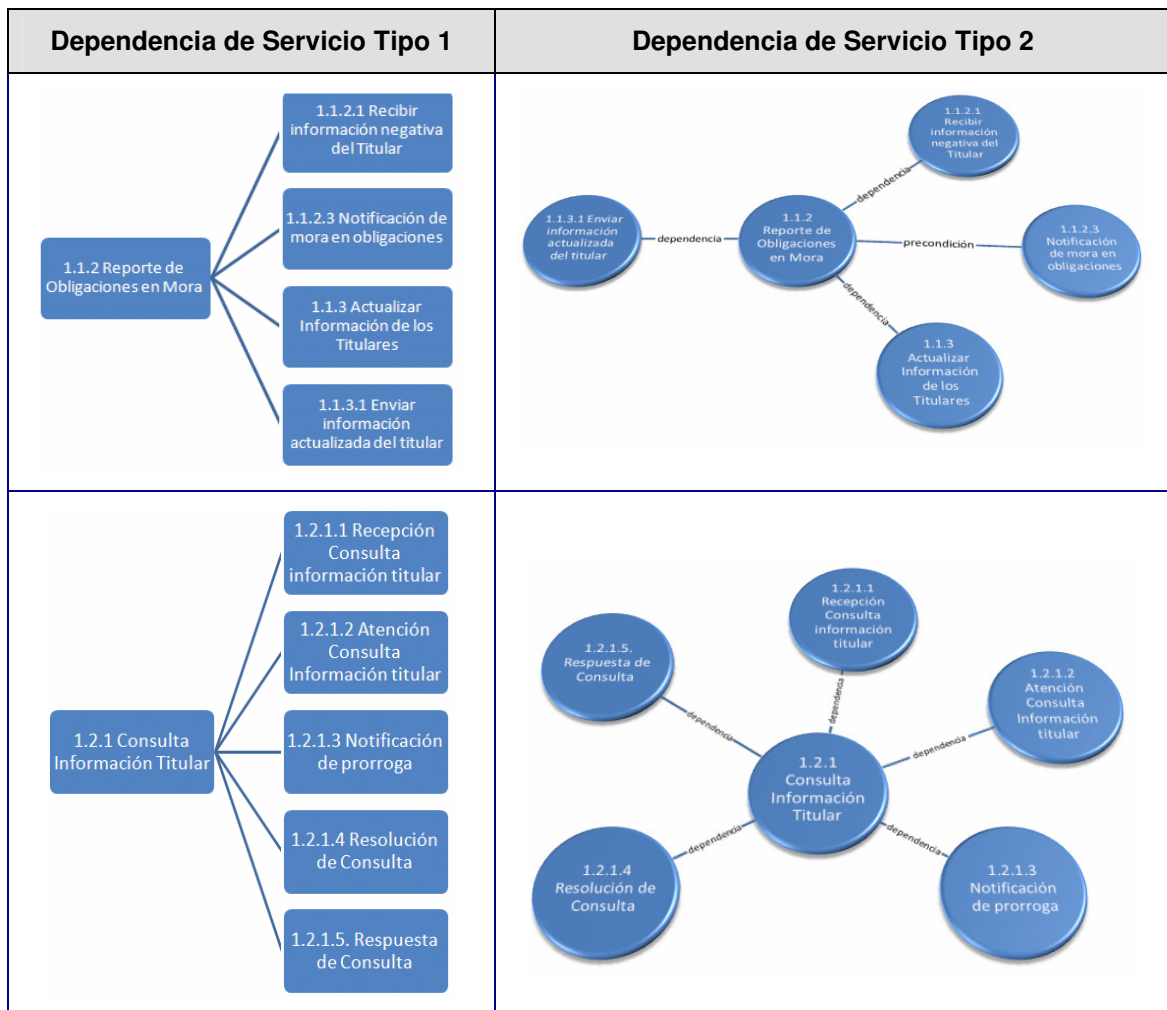
5.4 DEPENDENCIAS, COMPOSICIÓN Y FLUJO DE SERVICIOS

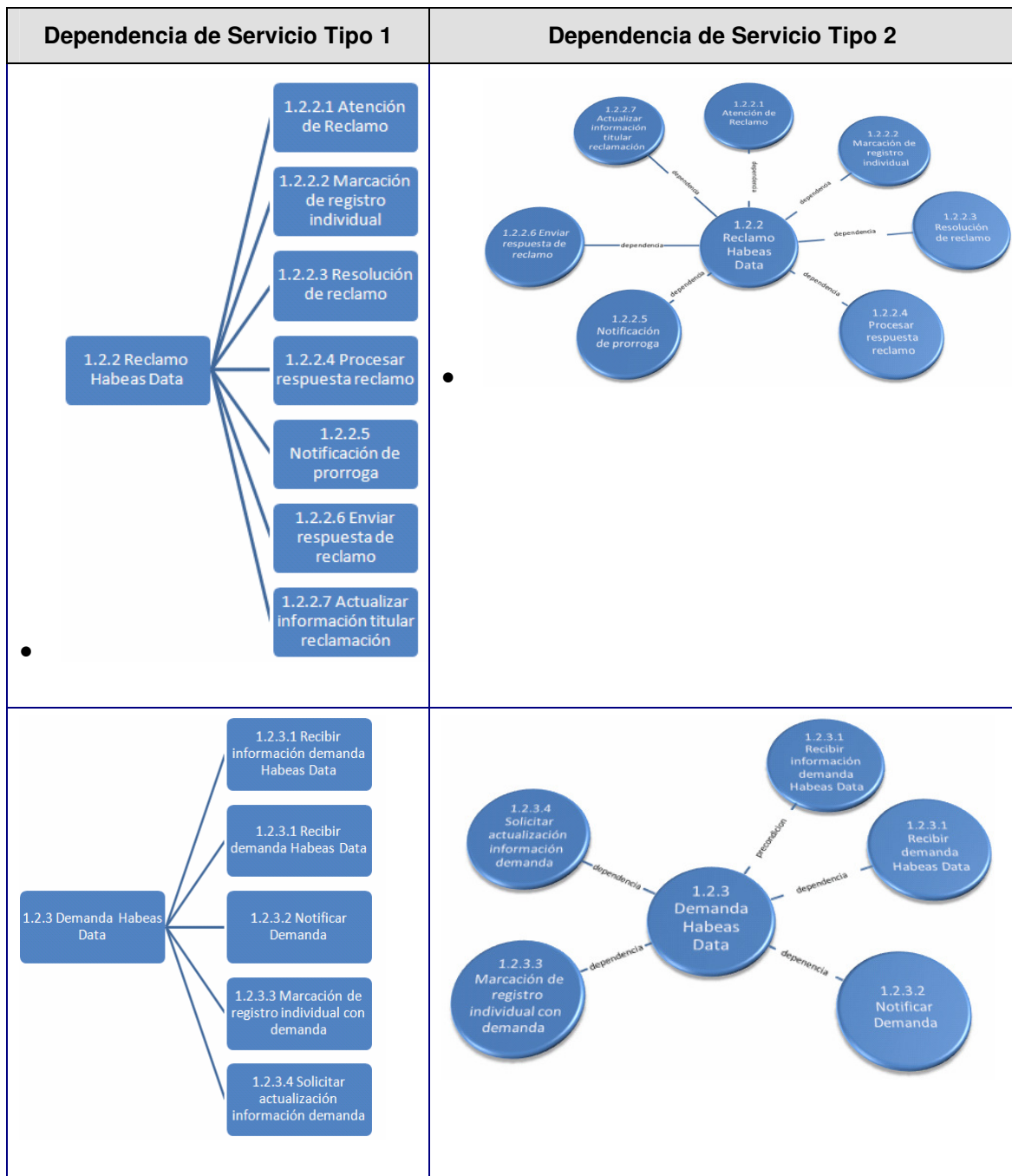
El modelado de la composición y dependencias de servicios, permite describir las relaciones existentes entre los servicios expuestos y que son utilizados a partir de un proceso de negocio, lo que implica una secuencia de ejecución de los servicios. Las relaciones de dependencia (que un servicio sólo se puede iniciar cuando otro ya se hubiera ejecutado con anterioridad) y de compensación (un servicio para su ejecución envuelve o requiere la instanciación de otros servicios subyacentes) son descritas en dos tipos de esquemas:

- Dependencias funcionales ("Tipo 1"): composición se deriva de múltiples servicios.
- Tiempo de dependencia ("Tipo 2"): Se determinan las precondiciones o requisitos para las composiciones o coreografías de servicios.

Tabla 36: Dependencias entre servicios







5.5 REQUERIMIENTOS NO FUNCIONALES DE SERVICIOS

RUP – SOMA recomienda simplificar la validación de los requisitos no funcionales para la validación de los servicios candidatos a implementación, por lo cual no se centra en todos los atributos de calidad definidos por la ISO 9126 [40], sino que define cuatro requisitos básicos que se deben evaluar al momento de realizar el modelado de servicios:

- Disponibilidad – MTBF (Medium Time Between Failures), MTTR (Medium Time To Repair).
- Ventana Operacional - es un tiempo en el cual los servicios no están disponibles para ser utilizados
- Tiempo de respuesta- la rapidez con la que un servicio debe responder a una solicitud.
- Pico de rendimiento (cuantos requerimientos para el servicio pueden llegar por unidad de tiempo, por ejemplo: por segundo, por minuto, por hora).

La entidad que use este marco de referencia arquitectónico para la implementación de la Ley Habeas Data, debe establecer los niveles de acuerdo de servicios las áreas funcionales y técnicas, de manera que se pueda dar respuesta a los objetivos estratégicos de la empresa y sus políticas de calidad.

Según la naturaleza de la entidad los niveles de acuerdo de servicio (SLA) y los requerimientos no funcionales definidos para el modelado de componentes de servicio, pueden utilizar diferentes atributos de calidad requeridos y no es necesario ajustarse únicamente a los propuestos por RUP -SOMA.

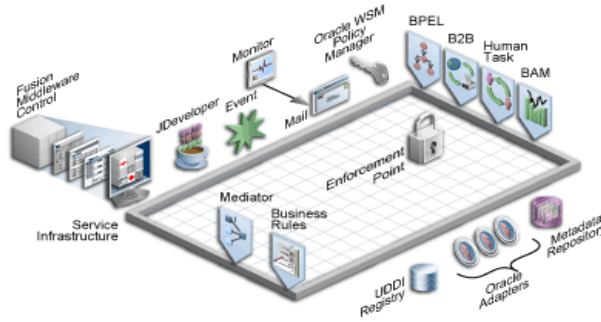
6 ARQUITECTURA TÉCNICA

El mercado de tecnología tiene múltiples opciones para la implementación de infraestructura que soporte el paradigma de Orientación a Servicio. De manera básica, todas las casas de tecnología deben manejar los siguientes componentes que soporten las siguientes funciones:

- Gestión de Key Performance Indicator (KPI) e implantación de tableros de control (Dashboard).
- Adaptadores: Conectividad a sistemas legados
- SOA testing (funcionalidad y desempeño): Servicios y procesos de negocio
- Registro de Servicios (UDDI): Modelo de Datos, WSDL, versiones
- Gobernabilidad SOA: Administración de cambio, ciclo de vida de servicios, gestión de versiones de servicios, soporte y mantenimiento de la calidad.

6.2 PROPUESTA DE TECNOLOGÍAS SOA

6.2.1 Tecnología Oracle



Fuente: [33]

Ilustración 15: Componentes de Oracle SOA Suite

Oracle SOA Suite permite el modelado de servicios, integración y gobernabilidad.

Comprende múltiples componentes de infraestructura de servicios que permiten diseñar, definir, administrar e integrar procesos del negocio.

Con la implantación de SOA las organizaciones pueden ampliar y adoptar bajo una misma plataforma múltiples arquitecturas internas sin necesidad de reemplazarlas.

SOA permite mayor calidad del servicio al interpretar los servicios en una arquitectura *grid* para escalabilidad y disponibilidad del servicio. Posee meta información, cumple estándares y niveles de servicio.

La infraestructura de SOA evoluciona a medida que se despliegan mas servicios y esta compuesta de manera general por:

- **Oracle BPEL Process Manager.** Habilita la integración empresarial de aplicaciones y servicios web multiplataforma en los procesos de negocio.
- **Oracle Web Services Manager.** Ofrece una solución para manejo de políticas de administrativas y servicios de seguridad de la infraestructura. Este provee visibilidad y control de las políticas a través de una administración centralizada
- **Oracle Business Rules.** Direcciona los requerimientos según las reglas del negocio para un tratamiento ágil, controlado y transparente
- **Oracle Business Activity Monitoring.** Efectúa monitoreo y planificación de las actividades del negocio, y establece líneas base de operación a través de la recolección de estadísticas.
- **Oracle Enterprise Service Bus.** Es un componente fundamental, provee frameworks de acoplamiento para mensajería entre aplicaciones. Integración aplicaciones multiplataforma sin ser intrusiva.
- **Oracle Service Registry.** Extiende el core UDDI (Universal Description, Discovery and Integration)V3 estándar con una única funcionalidad para publicar, categorizar y descubrir servicios Web.
- **Oracle JDeveloper.** Plataforma de desarrollo estándar para simplificar la creación de aplicaciones disponiendo de un entorno gráfico y declarativo, un entorno de codificación avanzado y estándar.

6.2.2 Tecnología IBM

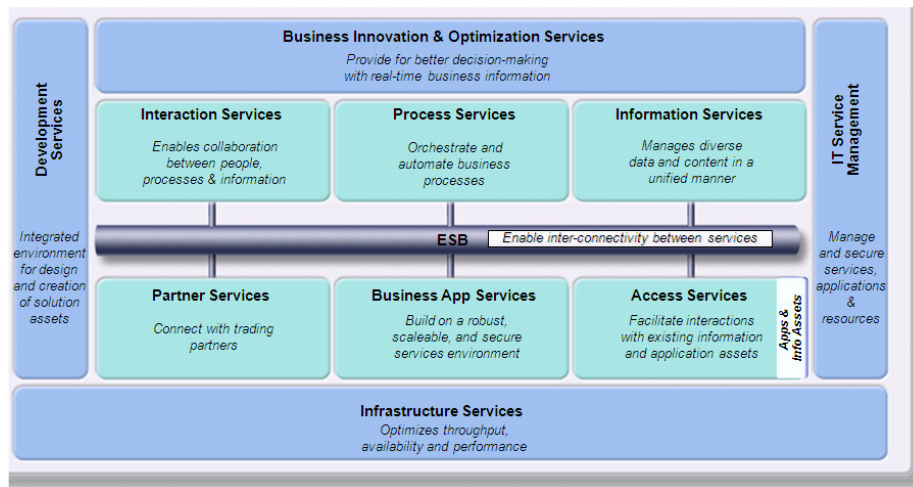
Los procesos de negocio en el contexto de una SOA se ejecutan bajo el control de un motor o servidor de procesos tal como el **WebSphere Process Server**. Existen además diversos componentes de middleware que facilitan la creación de nuevos servicios, la integración de los procesos con servicios nuevos o ya existentes y la interacción de los servicios y procesos con las personas.

En la visión propuesta por IBM estos componentes se clasifican del siguiente modo:

- Servicios de conectividad, que se implementan, como ya se ha dicho, mediante un patrón de Enterprise Service Bus (ESB).
- Servicios de negocio, que pueden ser dados por:
 - Nuevos componentes aplicativos, diseñados específicamente para una SOA y desarrollados por ejemplo en J2EE y ejecutarse bajo el servidor de aplicaciones WebSphere Application Server.
 - IBM provee para el desarrollo de estos nuevos componentes los productos de la plataforma IBM Rational que cubren todo el ciclo de vida de las aplicaciones.
 - Componentes aplicativos preexistentes, que pueden integrarse a una SOA, como se ha dicho antes, a través de adaptadores tales como los WebSphere Adapters provistos por IBM.
 - Servicios provistos por terceros. En las comunicaciones B2B se ha utilizado históricamente una gran variedad de protocolos (EDI, RosettaNet, FTP, Web Services, etc).
 - Para aislar a los aplicativos y procesos de la complejidad de manejar todos esos diferentes protocolos, y para manejar desde un lugar único cosas tales como la seguridad y los niveles de servicio, es conveniente contar con un gateway, que provea una interfaz de servicios a los aplicativos y procesos de la empresa y que se ocupe de manejar la comunicación con los diferentes proveedores de servicios externos. En la arquitectura SOA de IBM el componente que cubre esta función es el WebSphere Partner Gateway.
 - Elementos de control de los servicios, que incluyen:
 - Servidor de procesos, el WebSphere Process Server ya mencionado y del cual hablaremos detalladamente más adelante.

- Servidor de portal, que facilita la integración a nivel de la interfase de usuarios de los diferentes aplicativos y procesos. En la arquitectura SOA de IBM esta funcionalidad la brinda el WebSphere Portal Server.
- Servicios de integración de la información, que permiten visualizar fuentes de datos diversas como si fuesen una única base de datos. Esta funcionalidad la provee el WebSphere Information Integrator.

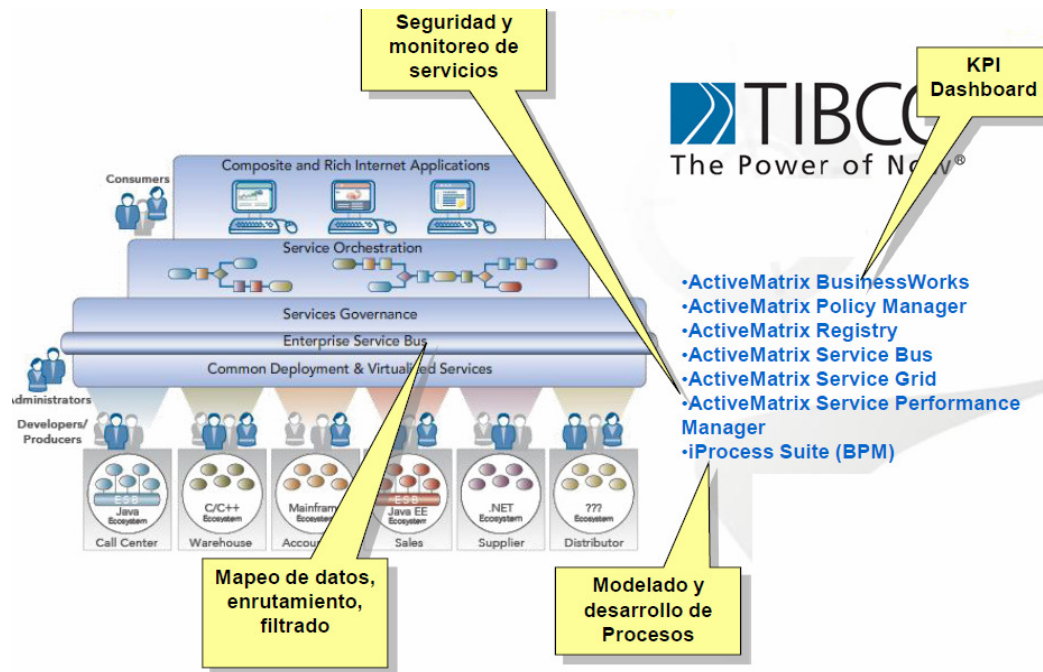
Todos estos elementos hacen parte de la Arquitectura SOA de Referencia de IBM, que se esquematiza del siguiente modo:



Fuente: [34]

Ilustración 16: Arquitectura de referencia SOA de IBM

6.2.3 Tecnología TIBCO



Fuente: [35]

Ilustración 17: Arquitectura SOA de Tibco

- **Tibco EMS:** Tibco Enterprise Message Server es la implementación del estándar JMS de Java de Tibco. Sobre este servidor recae la responsabilidad de transporte y enrutamiento del ESB previsto para la arquitectura SOA.
- **Tibco iProcess Engine:** Tibco iProcess Engine es el motor BPM de la suite de productos Tibco. Permite la ejecución de procesos de negocio de larga duración, y la orquestación de servicios y tareas que requieran interacción humana.

El servidor consta de varios procesos corriendo para cubrir las distintas partes de la funcionalidad. Entre ellos los workers, encargados de ejecutar los procesos, se pueden aumentar en número, siendo por tanto el servidor suficientemente escalable en este aspecto.

- **Tibco Business Factor y Tibco iProcess Insight:** Tibco Business Factor y Tibco iProcess Insight permite la monitorización de la actividad de negocio

(BAM) dentro de la arquitectura prevista. Tibco iProcess Insight es una extensión de Tibco Business Factor y permite la monitorización dentro de los workflows de iProcess.

- **Tibco Active Matrix Policy:** Los Web Services desarrollados con las herramientas y desplegados en los dominios existentes dentro de la SOA es necesario asegurarlos. Esta labor se realiza de una manera independiente de los desarrollos, por lo que para dotarlos de capacidades de aseguramiento de la información no es necesario cambiar en ningún aspecto el desarrollo original. El producto utilizado por Tibco para el aseguramiento de Web Services es Tibco Active Matrix Policy. Se trata de dos productos:
 - Tibco Active Matrix Policy Manager
 - Tibco Active Matrix Policy Agent

7 CONCLUSIONES

Al dar inicio a este trabajo fue necesario hacer varios re-planteamientos conceptuales: ¿qué es una arquitectura empresarial? ¿Cómo puede plantearse un modelo metodológico para implementar una arquitectura empresarial pero sin ser específica para una entidad financiera en particular? ¿Cómo abstraer de una ley, planteada lógicamente en términos legales, el marco referencial para su comprensión y concepción a nivel técnico? Como no caer en interpretaciones erradas? ¿Cómo establecer una nueva estructura arquitectónica que armonice con la arquitectura ya establecida mediante la disposición de múltiples elementos tecnológicos?

Para abordar este tema de la manera apropiada fue necesario conformar un grupo multidisciplinario, que como ejercicio académico participo en este proceso de manera algo fraccionada pero totalmente relevante para discusión requerida. Un abogado experto en el tema de legislación financiera, analistas expertos en el negocio financiero, arquitectos de software, arquitectos de soluciones empresariales, y algunas otros analistas con experiencia en la metodología de implementación de este tipo de legislaciones a nivel corporativo fueron las personas con las cuales pudo abstraerse todos los datos requeridos para definir la estructura arquitectónica expuesta en este trabajo.

Inicialmente la premisa era agilidad, como establecer la arquitectura requerida para adoptar la ley a través de un framework liviano (XAF) pero con la robustez obligada para este tipo de soluciones, pero durante el desarrollo del proyecto se llega a la conclusión que, más allá del framework elegido, más allá de la notación con la cual se trabaja, está la absoluta claridad de cómo opera el negocio, con un entendimiento real de los flujos de información, de los procesos y que estos estén 'escritos' y sean conocidos por la organización. Cualquier metodología es tan ágil como se quiera, algunas más prácticas para determinados nichos como el financiero, pero al final es el conocimiento del negocio, la disciplina en la documentación y un abogado especialista en el sector los que confluyen en una metodología técnica real, aplicable, estándar y, aunque inicialmente puede no ser óptima, que constituye la primera fase para alcanzar la convergencia de servicios en una arquitectura empresarial integrada.

Por increíble que parezca el primer problema y el más complicado de resolver es que las organizaciones no tienen procesos definidos, no están establecidos en lineamientos. Estos existen, claro, pero inmersos en las funcionalidades, en las

aplicaciones, en el día a día de las organizaciones. Así que fue necesario hacer el esfuerzo de retomar el conocimiento de los analistas del negocio, leer sobre estándares del mercado, y recopilar documentación de las aplicaciones operativas para establecer los procesos básicos y formular de allí la arquitectura del negocio. Esta fase, la más importante, y para este caso, engorrosa, facilitó el desarrollo de las demás arquitecturas planteadas dentro de la estructura propuesta. Sin la definición de los procesos no es posible la formulación de la arquitectura ni de ninguna metodología en este sentido.

Para las fases siguientes, el trabajo fue de ingeniería: plasmar lo planteado en la fase inicial más la interpretación de la ley a nivel tecnológico.

El producto acá desarrollado es el marco de referencia para una arquitectura orientada a servicios basado en TOGAF, XAF (Framework Arquitectura Extrema) y RUP-SOMA y se modela bajo el concepto MDA (Model Driven Architecture). El uso de MDA garantiza que la funcionalidad es definida en modelos independientes de la plataforma (Platform-Independent Model o PIM) usando UML, permitiendo a cualquier organización adaptar fácilmente la estructura arquitectónica a su propia infraestructura tecnológica, generando modelos de plataforma específica (Platform-Specific Model o PSM), además la notación UML es el modelo para el trabajo de XAF.

La visión específica del impacto en los flujos de trabajo permite el despliegue del modelo conceptual de la Ley Habeas Data, la definición de los macroprocesos y procesos derivados, casos de uso relevantes, detalle y jerarquización de servicios, el ciclo de vida de la información, el modelo canónico de datos, que a simple vista parece 'obvio' pero que en realidad ayuda ostensiblemente a las implementaciones técnicas y a la definición de las integraciones críticas, y en general la traducción de las especificaciones legales en un modelo integrado de servicios.

Por tratarse de un estudio académico, y aunque adaptado completamente a las necesidades puntuales de las organizaciones financieras, no se ha implementado en una corporación específica, sin embargo el desarrollo de cada fase fue validado con arquitectos de software IBM proveedores del grupo Aval, arquitectos empresariales de Banco de Occidente y con consultores internacionales expertos de Oracle para la implantación de soluciones iFlex.

Los estudios académicos en el sector financiero tienen un factor de riesgo difícil de aceptar: la confidencialidad. Este sector de la industria es especialmente celoso, y no sin razón, de la seguridad de la información (precisamente lo que propende leyes como Habeas Data), por lo que un estudio de este tipo en el cual se desglosan procesos internos y se hace muy legible su trazabilidad e impacto no son precisamente fáciles de desarrollar. Sin embargo, el uso de metodologías de arquitectura empresarial como una herramienta para poder construir un marco de referencia aplicable a una industria, que pueda ser usado y refinado por cualquier empresa financiera, tiene aceptación y es visualizado como un estándar que debe adoptarse en el sector.

Cuando un arquitecto empresarial del sector financiero lea este trabajo, tendrá un mayor entendimiento de la arquitectura de servicios que requiere para implementar la Ley Habeas Data y moldearla a su estructura organizacional, y aunque el estudio es específico para esta ley, le dará luces para la implementación de leyes similares, la receta que debe seguir para el correcto análisis de las mismas, y aunque se sumerja en el aprendizaje y adhesión de otros frameworks y otras tendencias tendrá un norte claro para la adecuación de la normatividad legal a las necesidades empresariales.

GLOSARIO

ARQUITECTURA CONTROLADA POR MODELOS (MDA): La OMG [1] la define de la siguiente manera: "Enfoque de la especificación de sistemas IT que separa la especificación de la funcionalidad de la especificación de la implementación de esa funcionalidad en una plataforma de tecnología específica" [11].

ARQUITECTURA EMPRESARIAL: La arquitectura empresarial es un conjunto de elementos organizado con relaciones claras entre sí, que juntos forman un todo definido por su funcionalidad. Los elementos representan la estructura organizativa y de comportamiento, y muestran las abstracciones de los procesos y estructuras clave de la empresa [11].

ARQUITECTURA ORIENTADA A SERVICIOS (SOA): Una arquitectura orientada a servicios define el conjunto de servicios que componen un sistema, describe las interacciones que se producen entre ellos para llevar a cabo determinado comportamiento, y correlaciona los servicios en una o más implementaciones de tecnologías específicas [11].

ARQUITECTURA: Concepto de sistema en su entorno, de nivel superior, de acuerdo con IEEE. La arquitectura de un sistema de software (en un momento dado del tiempo) es la organización o la estructura de los componentes importantes que interactúan mediante interfaces, con componentes compuestos de interfaces y componentes cada vez más pequeños [11].

ARTEFACTO: Un producto de trabajo formal que una tarea produce, modifica o utiliza, define un área de responsabilidad y está sujeto al control de versión. Un artefacto puede tener diversas formas, incluido un modelo, un elemento de modelo o un documento [11].

CENTRAL DE INFORMACIÓN FINANCIERA (CIFIN): CIFIN es un servicio privado de recolección, almacenamiento, procesamiento, administración, divulgación y cesión de información, conformado por bases de datos de diverso carácter, a través de las cuales se muestra el comportamiento comercial y financiero de las personas que son reportadas a ellas [4].

DATA CREDITO: DataCrédito es una central de información financiera y crediticia que administra información financiera, crediticia, comercial y de servicios relativa a la forma como las personas y las compañías han cumplido con sus obligaciones de crédito [5].

MODELADO EMPRESARIAL: Agrupa todas las técnicas de modelado que puede utilizar para modelar visualmente una empresa. Éstas son un subconjunto de las técnicas que puede utilizar para realizar ingeniería empresarial [11].

MODELO ESPECÍFICO DE PLATAFORMA (PLATFORM SPECIFIC MODEL – PSM): El OMG lo define de la siguiente manera: "Modelo de un subsistema que incluye información sobre la tecnología específica que se utiliza en su ejecución en una plataforma específica, y posiblemente contenga elementos específicos de esa plataforma" [17].

MODELO INDEPENDIENTE DE PLATAFORMA (PLATFORM INDEPENDENT MODEL – PIM): El OMG lo define de la siguiente manera: "Modelo de un subsistema que no contiene información específica de la plataforma ni de la tecnología que se utiliza para llevarlo a cabo" [17].

MODELO: Descripción completa de un sistema desde una perspectiva determinada (completa significa que no es necesario añadir información adicional para comprender el sistema desde dicha perspectiva) [11].

PATRÓN DE ARQUITECTURA: "Un patrón de arquitectura expresa un esquema de organización estructural fundamental para sistemas de software. Proporciona un conjunto de subsistemas predefinidos, especifica sus responsabilidades e incluye reglas y directrices para organizar las relaciones entre ellos" [11].

RUP: Rational Unified Process

SERVICIO (EN CONTEXTO DE SOA): Un servicio es un recurso de software que puede ser descubierto con una especificación de software ubicada en una ruta externa. Esta especificación de servicio está disponible para la búsqueda, el enlace y la invocación mediante un consumidor de servicios. El proveedor de servicios realiza la implementación de especificación de servicio y también ofrece la calidad de requisitos de software al consumidor de servicios. Los servicios están regidos por políticas declarativas y, por tanto, dan soporte al estilo de arquitectura dinámicamente reconfigurable [11].

UML (Lenguaje unificado de modelado): Lenguaje de visualización, especificación, construcción y documentación de artefactos de un sistema de software intensivo [11].

VISTA ARQUITECTÓNICA: Vista arquitectónica del sistema desde una perspectiva determinada. Se centra principalmente en la estructura, la modularidad, los componentes fundamentales y los flujos de control principales [11].

8 BIBLIOGRAFÍA

- [1] THE OPEN GROUP. The Open Group Architecture Framework (TOGAF). Version 8. 'Enterprise Edition. {En línea}. {2002} disponible en: www.opengroup.org/products/publications/catalog/i912.htm)
- [2] SAHA, Pallab. Handbook of Enterprise Systems Architecture in Practice. IGI Global. 2007
- [3] ROBINSON, Phil y GOUT, Floris. XAF: A Minimalist EA Framework for an Agile Environment. Cutter IT Journal. Volumen 19. Número 3. {En línea}. {Marzo 2006} disponible en: <http://www.extremearchitecture.org>
- [4] CIFIN. Asobancaria. {En línea}. {2005} disponible en: <http://cifin.asobancaria.com>).
- [5] COMPUTEC S.A., Datacrédito. {En línea}. {2009} disponible en: www.datacredito.com.co).
- [6] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Anexo Carta Circular 31 de 2002.
- [7] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley estatutaria 1266 del 31 de diciembre de 2008. Habeas Data. Bogotá D.C., Colombia. 2008.
- [8] IEEE 90: IEEE Standard Glossary of Software Engineering Terminology.
- [9] HOHPE, Gregor and WOOLF, Bobby. Enterprise Integration Patterns.
- [10] SAP. Estrategias para un crecimiento rentable en el sector Financiero. Catálogo de preventa. Enero de 2009.
- [11] IBM. Rational Unified Process (RUP). Modelado de Servicio. Versión 7.2.0

- [12] Wahli, Ueli et al: "Building SOA Solutions Using the Rational SDP". IBM Redbooks, 2007.
- [13] ERL, Thomas: "Service-Oriented Architecture (SOA): Concepts, Technology, and Design". Prentice Hall, 2005.
- [14] "SOA Immersion for EDS". Web Age Solutions, 2007.
- [15] "SOA Course Introduction". Electronic Data Systems, 2007.
- [16] PoT de SOA y governance con herramientas IBM. IBM Colombia. 2009.
- [17] OBJECTMANAGEMENT GROUP, "MDA Guide Version1.0.1", 2003
- [18] Kleppe, Anneke; Warmer, Jos; Bast, Wim. "MDA Explained: The Model Driven Architecture™: Practice and Promise". AddisonWesley, 2003.
- [19] Constitución Política de Colombia 1991. Editorial Leyer. Bogota 2005.
- [20] The APM Group Limited, Sword House, Totteridge Road, High Wycombe, Buckinghamshire, UK, HP13 6DG. Prince2. {En línea}. {2009} disponible en: (<http://www.prince-officialsite.com/home/home.asp>).
- [21] THE OPEN GROUP. The Open Group Architecture Framework (TOGAF). Version 9. 'Enterprise Edition. {En línea}. {2009} disponible en: (<http://www.opengroup.org/architecture/togaf9-doc/arch/chap35.html>).
- [22] W3C. The World Wide Web Consortium. XML Schema Definition. Versión 1.1. {En línea}. {2009} disponible en: (<http://www.w3.org/XML/Schema>).
- [23] W3C. The World Wide Web Consortium. XSL Transformations (XSLT). Versión 1.0. {En línea}. {2009} disponible en: (<http://www.w3.org/TR/1999/REC-xslt-19991116>).

- [24] Network Working Group. SolidMatrix Technologies, Inc. Common Format and MIME Type for Comma-Separated Values (CSV) Files. {En línea}. {2005} disponible en: (<http://tools.ietf.org/html/rfc4180>).
- [25] EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES. Copybook models and handwriting samples database. {En línea}. {2008} disponible en: (<http://www.enfsi.eu/page.php?uid=76>).
- [26] OASIS. Organization for the Advancement of Structured Information Standards. Web Services Business Process Execution Language (WSBPEL) TC. {En línea}. {2009} disponible en: (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsBPEL).
- [27] FEW, Stephen. Information Dashboard Design. O'Reilly. 2006. ISBN 978-0-596-10016-2.
- [28] PARMENTER, David. Key Performance Indicators. John Wiley & Sons. 2007. ISBN 0-470-09588-1.
- [29] LINTHICUM, David S. SOA Watch: SOA and Adapters. SOA Institute. {En línea}. {2008} disponible en: (<http://www.soainstitute.org/articles/article/article/soa-watch-soa-and-adapters.html>).
- [30] TORRY HARRIS BUSINESS SOLUTIONS. SOA Test Methodology. {En línea}. {2007} disponible en: (http://www.thbs.com/pdfs/SOA_Test_Methodology.pdf).
- [31] OASIS. Organization for the Advancement of Structured Information Standards. UDDI Specification TC. {En línea}. {2009} disponible en: (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec).
- [32] ORACLE. Oracle SOA Suite 11g. {En línea}. {2009} disponible en: (<http://www.oracle.com/technologies/soa/soa-suite.html>).
- [33] ORACLE. Oracle WebLogic Suite 11g. {En línea}. {2009} disponible en: (<http://www.oracle.com/appserver/weblogic/weblogic-suite.html>).

- [34] IBM. IBM WebSphere SOA Suite. {En línea}. {2009} disponible en: (<http://www-01.ibm.com/software/websphere>).
- [35] TIBCO. Service-Oriented Architecture (SOA) Resource Center. {En línea}. {2009} disponible en: (<http://www.tibco.com/solutions/soa/default.jsp>).
- [36] MICROSOFT. BizTalk Server. {En línea}. {2009} disponible en: (<http://www.microsoft.com/biztalk/en/us/default.aspx>).
- [37] Codigo Industrial Internacional Uniforme (CIIU). {En línea}. {2009} disponible en: (<http://www.contabilidad.com.co/ciiu.html>).
- [38] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 052 del 2007. Bogotá D.C., Colombia. 2007.
- [39] SIRE – Sistema de Información de Reclamos. Asobancaria. Manual Técnico. Versión 1.0
- [40] ISO/IEC 9126 and 14598 integration aspects: A Brazilian viewpoint. The Second World Congress on Software Quality, Yokohama, Japan, 2000.
- [41] THE OPEN GROUP. Business Process Management Notation (BPMN). Version 1.2. {En línea}. {2009} disponible en: (<http://www.bpmn.org>).
- [42] GARTNER. Gartner Magic Quadrant. {En línea}. {2009} disponible en: (<http://www.gartner.com>).